

# **Oracle® Retail Returns Management**

Installation Guide

Release 2.1

July 2009

Copyright © 2009, Oracle. All rights reserved.

Primary Author: Bernadette Goodman

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

## Value-Added Reseller (VAR) Language

### Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

- (i) the software component known as **ACUMATE** developed and licensed by Lucent Technologies Inc. of Murray Hill, New Jersey, to Oracle and imbedded in the Oracle Retail Predictive Application Server - Enterprise Engine, Oracle Retail Category Management, Oracle Retail Item Planning, Oracle Retail Merchandise Financial Planning, Oracle Retail Advanced Inventory Planning, Oracle Retail Demand Forecasting, Oracle Retail Regular Price Optimization, Oracle Retail Size Profile Optimization, Oracle Retail Replenishment Optimization applications.
- (ii) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.
- (iii) the **SeeBeyond** component developed and licensed by Sun Microsystems, Inc. (Sun) of Santa Clara, California, to Oracle and imbedded in the Oracle Retail Integration Bus application.
- (iv) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.
- (v) the software component known as **Crystal Enterprise Professional and/or Crystal Reports Professional** licensed by SAP and imbedded in Oracle Retail Store Inventory Management.
- (vi) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.
- (vii) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.
- (viii) the software component known as **Style Report™** developed and licensed by InetSoft Technology Corp. of Piscataway, New Jersey, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.
- (ix) the software component known as **DataBeacon™** developed and licensed by Cognos Incorporated of Ottawa, Ontario, Canada, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.



---

---

# Contents

<b>Preface</b> .....	xiii
Audience.....	xiii
Related Documents .....	xiii
Customer Support .....	xiii
Review Patch Documentation .....	xiv
Oracle Retail Documentation on the Oracle Technology Network .....	xiv
Conventions .....	xiv
 <b>1 Preinstallation Tasks</b>	
<b>Check Database Server Requirements</b> .....	1-1
Required Settings for Database Installation .....	1-2
Secure JDBC with Oracle 11g .....	1-2
<b>Check Application Server Requirements</b> .....	1-2
Install Required Patches for the Oracle Stack .....	1-2
Check for SSL Certificate.....	1-3
<b>Check Java Key Store Requirement</b> .....	1-3
<b>Hardware Requirements</b> .....	1-4
<b>Check Client PC and Web Browser Requirements</b> .....	1-4
<b>Uptake Installation</b> .....	1-4
 <b>2 Installation of the Oracle Stack on OEL</b>	
Create a New OC4J Instance for Returns Management.....	2-1
Create the Database Schema Owner and Data Source Users .....	2-2
Expand the Returns Management Distribution .....	2-3
Obtain Third-Party Library Files Required by Returns Management .....	2-4
Installation Options .....	2-5
Database Install Options .....	2-5
Secure the JDBC for the Oracle 11g Database .....	2-6
Install the Java Cryptography Extension (JCE) .....	2-7
Run the Returns Management Application Installer.....	2-7
Resolving Errors Encountered During Application Installation .....	2-8
Oracle Configuration Manager.....	2-9
Backups Created by Installer .....	2-9
Manual Deployment of the Key Store .....	2-9

Install Parameters Option.....	2-10
Manual Deployment of the Returns Management Application .....	2-10
Import Initial Parameters.....	2-11
Importing Parameters Through the User Interface.....	2-11
Importing Parameters By Using an Ant Target.....	2-11
Load Optional Purge Procedures .....	2-12
Using the Returns Management Application .....	2-12

### **3 Installation of the IBM Stack on IRES**

Check the WebSphere Application Server Settings .....	3-1
Authentication Cache Timeout .....	3-1
Create the Database Schema Owner and Data Source Users .....	3-1
Expand the Returns Management Distribution .....	3-2
Obtain Third-Party Library Files Required by Returns Management .....	3-3
Securing the JDBC for the IBM DB2 Database .....	3-3
Install the Java Cryptography Extension (JCE) .....	3-4
Installation Options.....	3-4
Database Install Options .....	3-5
Run the Returns Management Application Installer.....	3-6
Resolving Errors Encountered During Application Installation .....	3-7
Oracle Configuration Manager.....	3-7
Manual Deployment of the Key Store .....	3-8
Configure IBM WebSphere MQ.....	3-8
Manual Deployment of the Returns Management Application .....	3-9
Install Parameters .....	3-10
Import Initial Parameters.....	3-10
Importing Parameters Through the User Interface.....	3-10
Importing Parameters By Using an Ant Target.....	3-11
Load Optional Purge Procedures .....	3-11
Using the Returns Management Application .....	3-11

### **A Appendix: Returns Management Application Installer Screens for the Oracle Stack**

### **B Appendix: Returns Management Application Installer Screens for the IBM Stack on IRES**

### **C Appendix: Installer Silent Mode**

### **D Appendix: Reinstalling Returns Management**

Reinstalling Returns Management on the Oracle Stack.....	D-1
Reinstalling Returns Management on the IBM Stack .....	D-1

### **E Appendix: URL Reference**

URLs for the Oracle Stack.....	E-1
JDBC URL for a Database .....	E-1

JNDI Provider URL for an Application .....	E-1
Deployer URI .....	E-2
<b>URLs for the IBM Stack .....</b>	<b>E-2</b>
JDBC URL for a Database .....	E-2
JNDI Provider URL for an Application .....	E-2
 <b>F Appendix: Common Installation Errors</b>	
Unreadable Buttons in the Installer .....	F-1
Installation Errors for the Oracle Stack.....	F-1
Oracle Application Server Forceful Shutdown.....	F-1
OC4J Instance Does Not Exist .....	F-1
OC4J Instance is Not Started .....	F-2
"Unable to get a deployment manager" Message.....	F-2
"Could not create system preferences directory" Warning.....	F-3
Installation Hangs at "Compiling EJB generated code" .....	F-3
"Failed to set the internal configuration" Message.....	F-3
 <b>G Appendix: Returns Data Loader</b>	
Using the Returns Data Loader .....	G-1
 <b>H Appendix: Best Practices for Passwords</b>	
Password Guidelines .....	H-1
Special Security Options for Oracle Databases.....	H-2
Enforcing Password Policies Using Database Profiles .....	H-2
Enforcing Password Policies Using a Verification Script.....	H-2
Special Security Options for IBM DB2 Databases .....	H-3
 <b>I Appendix: Secure JDBC with Oracle 11g Database</b>	
Creating the Oracle Wallet and Certificate for the Server.....	I-1
Securing the Listener on the Server.....	I-2
Examples of Network Configuration Files .....	I-2
listener.ora.....	I-3
sqlnet.ora .....	I-3
tnsnames.ora .....	I-3
Securing Client Access .....	I-4
Specific Instructions for Central Office.....	I-4
Configuring the Application Server Machine.....	I-4
Securing the Data Source .....	I-5
Creating a JDBC Shared Library for the Application .....	I-5
 <b>J Appendix: Secure JDBC with IBM DB2</b>	
Summary .....	J-1
Prerequisites .....	J-1
Setting up the Key Store .....	J-2
Creating a Self-signed Digital Certificate for Testing.....	J-2

Configuring the IBM DB2 Server .....	J-2
Exporting a Certificate from iKeyman .....	J-4
Configuring the IBM FIPS-compliant Provider for SSL (optional) .....	J-4
Configuring Central Office on IBM WebSphere .....	J-5
Useful Links .....	J-6

## **K Appendix: Installation Order**

Enterprise Installation Order .....	K-1
-------------------------------------	-----



## List of Figures

A-1	Introduction .....	A-1
A-2	Requirements.....	A-2
A-3	License Agreement .....	A-2
A-4	Database Owner .....	A-3
A-5	Data Source User .....	A-4
A-6	Enable Secure JDBC .....	A-5
A-7	Data Source SSL Configuration .....	A-5
A-8	Database Install Options .....	A-6
A-9	Default Locale.....	A-7
A-10	Returns Management Administrator User.....	A-7
A-11	Security Setup: Key Store.....	A-8
A-12	RSA Key Manager Requirements .....	A-9
A-13	Key Store Details for RSA Key Manager 2.1.3 .....	A-10
A-14	RSA Key Store Configuration .....	A-10
A-15	Key Store Details for Simulator Key Manager.....	A-12
A-16	Key Store Details for Other Key Manager.....	A-12
A-17	Deploy Key Store Connector RAR .....	A-13
A-18	Key Store Connector RAR Details .....	A-14
A-19	App Server ORACLE_HOME.....	A-15
A-20	Mail Session Details .....	A-15
A-21	Application Server Details.....	A-16
A-22	Manual Deployment Option .....	A-17
A-23	Application Deployment Details .....	A-18
A-24	Install Parameters Option .....	A-19
A-25	Application Server RMI Port.....	A-19
A-26	OC4J Administrative User.....	A-20
A-27	Installation Progress .....	A-21
A-28	Installation Complete .....	A-21
B-1	Introduction .....	B-1
B-2	Requirements.....	B-2
B-3	License Agreement .....	B-2
B-4	Database Owner .....	B-3
B-5	Data Source User .....	B-4
B-6	Enable Secure JDBC .....	B-5
B-7	Data Source SSL Configuration .....	B-5
B-8	Database Install Options .....	B-6
B-9	Default Locale.....	B-7
B-10	Returns Management Administrator User.....	B-7
B-11	Security Setup: Key Store .....	B-8
B-12	RSA Key Manager Requirements .....	B-9
B-13	Key Store Details for RSA Key Manager 2.1.3 .....	B-10
B-14	RSA Key Store Configuration .....	B-10
B-15	Key Store Details for Simulator Key Manager.....	B-12
B-16	Key Store Details for Other Key Manager.....	B-12
B-17	Deploy Key Store Connector RAR .....	B-13
B-18	Key Store Connector RAR Details .....	B-14
B-19	App Server WAS_HOME .....	B-15
B-20	Mail Session Details .....	B-15
B-21	Application Server Details.....	B-16
B-22	JMS Server Details.....	B-18
B-23	Configure MQ Server Option.....	B-19
B-24	MQ Server Directory .....	B-20
B-25	Manual Deployment Option .....	B-20
B-26	Application Deployment Details .....	B-21

B-27	Install Parameters Option .....	B-22
B-28	Installation Progress .....	B-22
B-29	Installation Complete .....	B-23

**List of Tables**

1-1	Database Server Component Versions Tested for this Release .....	1-1
1-2	Application Server Component Versions Tested for this Release .....	1-2



---

---

# Preface

Oracle Retail Installation Guides contain the requirements and procedures that are necessary for the retailer to install Oracle Retail products.

## Audience

This Installation Guide is written for the following audiences:

- Database administrators (DBA)
- System analysts and designers
- Integrators and implementation staff

## Related Documents

For more information, see the following documents in the Oracle Retail Returns Management Release 2.1 documentation set or the Oracle Retail Strategic Store Solutions Release 13.1.1 documentation set:

- *Oracle Retail Returns Management Release Notes*
- *Oracle Retail Returns Management Operations Guide*
- *Oracle Retail Returns Management User Guide*
- *Oracle Retail Strategic Store Solutions Configuration Guide*

## Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

- <https://metalink.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to recreate
- Exact error message received
- Screen shots of each step you take

## Review Patch Documentation

If you are installing the application for the first time, you install either a base release (for example, 13.1) or a later patch release (for example, 13.1.1). If you are installing a software version other than the base release, be sure to read the documentation for each patch release (since the base release) before you begin installation. Patch documentation can contain critical information related to the base release and code changes that have been made since the base release.

## Oracle Retail Documentation on the Oracle Technology Network

In addition to being packaged with each product release (on the base or patch level), all Oracle Retail documentation is available on the following Web site (with the exception of the Data Model which is only available with the release packaged code):

[http://www.oracle.com/technology/documentation/oracle\\_retail.html](http://www.oracle.com/technology/documentation/oracle_retail.html)

Documentation should be available on this Web site within a month after a product release. Note that documentation is always available with the packaged code on the release date.

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

---

## Preinstallation Tasks

This chapter describes the requirements that must be met before the Oracle Retail Returns Management application can be installed.

---

**Note:** The Oracle stack and IBM stack are the configurations that were tested for this release. The components required for each stack are listed in this chapter. For each component, the product and the version that were used for testing are included. While Returns Management may work in other configurations, these are the configurations that are tested for this release.

---

If you will be installing multiple Oracle Retail applications, see [Appendix K](#) for a guideline for the order in which the applications should be installed.

### Check Database Server Requirements

[Table 1–1](#) lists the general components required for a database server and the versions tested for this release.

**Table 1–1 Database Server Component Versions Tested for this Release**

Component	Oracle Stack	IBM Stack
Operating System	Oracle Enterprise Linux 5 Update 2 (OEL 5.2) for Linux x86-64	IBM IRES 2.1.5 SUSE Linux Enterprise Server 9
Database	Oracle Database 11g Enterprise Edition version 11.1.0.7 (64-bit)	IBM DB2 version 9.5 with fixpack 3b (64-bit)

## Required Settings for Database Installation

The following settings must be made during database creation:

- The database must be set to store data in UTF-8 encoding.
- When using the Oracle 11g database server, make the following changes to the system settings:

---

**Note:** These changes are only needed when using the Oracle 11g database server.

---

```
ALTER SYSTEM SET NLS_NUMERIC_CHARACTERS = '.,-' SCOPE=SPFILE;
ALTER SYSTEM SET NLS_DATE_FORMAT = 'YYYY-MM-DD' SCOPE=SPFILE;
ALTER SYSTEM SET NLS_TIMESTAMP_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF'
SCOPE=SPFILE;
```

## Secure JDBC with Oracle 11g

Creating the Oracle wallet and certificate for the server requires that the Advanced Security options are installed with the database server. For more information, see ["Secure the JDBC for the Oracle 11g Database"](#) in [Chapter 2](#).

## Check Application Server Requirements

[Table 1–2](#) lists the general components required for an application server capable of running Returns Management and the versions tested for this release.

**Table 1–2 Application Server Component Versions Tested for this Release**

Component	Oracle Stack	IBM Stack
Operating System	Oracle Enterprise Linux 5 Update 2 (OEL 5.2) for Linux x86-64	IBM IRES 2.1.5 SUSE Linux Enterprise Server 9 Patch Level 3
J2EE Application Server	Oracle Application Server 10g Enterprise Edition version 10.1.3.4  <b>Note:</b> This release of Returns Management is only supported in a managed OC4J instance as part of Oracle AS 10g. It is not supported on OC4J standalone.	IBM WebSphere 6.1.0.19
J2EE Application Server JVM	Sun JRE 1.5.0_06	IBM JRE 1.5.0
Messaging Provider	included in Oracle Application Server	IBM WebSphere MQ 6.0.2.5
System Management Agent	OEM 10.1.3.4	IBM WebSphere Admin Console 6.1.0.19

## Install Required Patches for the Oracle Stack

To use Oracle Application Server version 10.1.3.4 with an Oracle 11g database, you must apply patches to the OPatch utility and Oracle Application Server:

1. Download and install OPatch version 10.1.0.0.0 from ARU for your platform. The ARU Checkin number is 6880880.
2. Use OPatch to apply ARU Request Number 10579638.



## Check for SSL Certificate

Oracle Retail Returns Management is accessed through a secure HTTP connection. The installation of an SSL Certificate is required on your application server. If the certificate is not installed, warnings are displayed when trying to access Oracle Retail Returns Management.

For information on installing the SSL Certificate, refer to your application server documentation.

## Check Java Key Store Requirement

Oracle Retail Returns Management requires that a Java Key Store is created prior to installation. A Key Store connector RAR file is required to enable the connection between Oracle Retail Returns Management and the Key Store. During installation, the RAR file must be deployed to the application server. Specific information for configuring the Key Store and deploying the RAR file is entered on the Security Setup: Key Store installer screens.

If you are using the RSA Key Manager, you must use version 2.1.3 and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 5.0.

- For the Oracle stack, see ["Install the Java Cryptography Extension \(JCE\)" in Chapter 2.](#)
- For the IBM stack, see ["Install the Java Cryptography Extension \(JCE\)" in Chapter 3.](#)

Since Oracle Retail Returns Management does not use any secure data related to key management, the simulated key manager bundled with the application may be used.

---

---

**WARNING:** A simulated key management package is bundled with Oracle Retail Returns Management. It is not compliant with either the Payment Application Data Security Standard (PA-DSS) or Payment Card Industry Data Security Standard (PCI-DSS). It is made available as a convenience for retailers and integrators. If you use the simulated key manager, you will not be PCI-DSS compliant.

---

---

## Hardware Requirements

Specific hardware requirements for the machines running Oracle Retail Returns Management depend on variables including the number of users, number of stores and registers, transaction volume, returns data retention period, and other applications running on the same machine.

Please note the following about the hardware requirements:

- The CPU requirement depends on variables including the operating system and middleware selected.
- The memory requirements and performance depend on variables including the operating system and middleware selected.
- Disk size can vary based on the operating system and middleware requirements, as well as the amount of data storage needed. Data storage depends on variables including the data retention period and so on.

You need to determine your hardware requirements, based on the variables mentioned here, as well as any additional variables specific to your environment. For more information, contact Customer Support.

## Check Client PC and Web Browser Requirements

The general requirements for the client system include the following:

- Adobe Acrobat Reader or another application capable of rendering Portable Data Format (PDF) files

The following web browser was tested for this release:

- Microsoft Internet Explorer 6

## Uptake Installation

This installation guide details the steps needed to perform a full installation of Oracle Retail Returns Management Release 2.1. To assist in the uptake of Oracle Retail Returns Management from Release 2.0 to Release 2.1, tools are available on My Oracle Support.

The following document is available through My Oracle Support (formerly MetaLink). Access My Oracle Support at the following URL:

<https://metalink.oracle.com>

***Oracle Retail Upgrade Guide (Doc ID: 837368.1)***

This guide contains the following information:

- List of the impacts of the Release 2.1 functional changes on the database schema.
- Description of the tools available to assist in the uptake of the database and code.

---

## Installation of the Oracle Stack on OEL

---

Before proceeding, you must install the database and application server software. For a list of supported versions, see [Chapter 1](#).

During installation, the Returns Management database schema is created and the Returns Management application is deployed to an OC4J instance within the OracleAS 10g installation. The Java JDK that is included with the Oracle Application Server (under `$ORACLE_HOME/jdk`) will be used to run the application.

### Create a New OC4J Instance for Returns Management

You can skip this section if you are redeploying to an existing OC4J instance.

The Returns Management application must be deployed to its own dedicated OC4J instance. For instructions on how to create a new OC4J instance, see Adding and Deleting OC4J Instances in the Reconfiguring Application Server Instances chapter of the *Oracle Application Server Administrator's Guide*.

To create a new OC4J instance:

1. Log onto the server, which is running your OracleAS 10g installation, as the user who owns the OracleAS 10g installation. Set your `ORACLE_HOME` environment variable to point to this installation. You must use forward slash file separators when setting this variable, as shown in the following example.

```
ORACLE_HOME=/u01/oracle/product/10.1.3.4/OracleAS_1
```

2. Choose a name for the new OC4J instance. In the remainder of this installation guide, `<orrm-inst>` is used for the name..
3. Create this OC4J instance as documented in the *Oracle Application Server Administrator's Guide*, for example:

```
$ORACLE_HOME/bin/createinstance -instanceName <orrm-inst>  
-groupName <group name>
```

Including a group name is optional.

---

**Note:** When prompted for the oc4jadmin password, provide the same administrative password you gave for the OracleAS 10g installation. All OC4J instances running Oracle Retail applications must have the same oc4jadmin password.

---

---

**Note:** The `jms` and `rmi` port numbers should be set so that the numbers do not overlap between all the instances in your configuration. Also, a specific port number should be set rather than a range of port numbers. If a range of port numbers is specified, the same port number may not be used each time the instance is started.

The port numbers are defined in the `$ORACLE_HOME/opmn/conf/opmn.xml` file. The following is an example definition of the port numbers in that file.

Port number definitions for the home instance:

```
<port id="rmi" range="12401-12401"/>
<port id="jms" range="12601-12601"/>
<port id="rmis" range="12701-12701"/>
```

Port number definitions for the Returns Management instance:

```
<port id="rmi" range="12402-12402"/>
<port id="jms" range="12602-12602"/>
<port id="rmi" range="12702-12702"/>
```

---

4. Start the OC4J instance. You can do this through the Enterprise Manager web interface, or on the command line using the `opmnctl` utility:
  - a. `$ORACLE_HOME/opmn/bin/opmnctl start`
  - b. `$ORACLE_HOME/opmn/bin/opmnctl startproc  
process-type=<orrm-inst>`
5. Verify that the OC4J instance was fully started. If you are using the Enterprise Manager web interface, the instance should have a green arrow indicating that it is running. On the command line, verify that the instance has a status of "Alive".

```
$ORACLE_HOME/opmn/bin/opmnctl status
```

If you are unable to start the OC4J instance after several attempts, try increasing the startup timeouts in `$ORACLE_HOME/opmn/conf/opmn.xml`. If that does not help, consult the Oracle Application Server documentation for further assistance.

## Create the Database Schema Owner and Data Source Users

The following recommendations should be considered for schema owners:

- Database administrators should create an individual schema owner for each application, unless the applications share the same data. In the case of Oracle Retail Back Office and Point-of-Service, the database schema owner are the same because these applications share a database.
- The schema owners should only have enough privileges to install the database.

For information on best practices for passwords, see [Appendix H](#).

To create the database schema owner and data source users:

1. Log in using the database administrator user ID.
2. Create a role in the database to be used for the schema owner.

```
CREATE ROLE <schema_owner_role>;
```

3. Grant the privileges, shown in the following example, to the role.

```
GRANT CREATE TABLE, CREATE VIEW, CREATE SEQUENCE, CREATE PROCEDURE, ALTER
SESSION, CONNECT, SELECT_CATALOG_ROLE TO <schema_owner_role>;
```

4. Create a role in the database to be used for the data source user.

```
CREATE ROLE <data_source_role>;
```

5. Grant the privileges, shown in the following example, to the role.

```
GRANT CONNECT, CREATE SYNONYM, SELECT_CATALOG_ROLE TO
<data_source_role>;
```

6. Create the schema owner user in the database.

```
CREATE USER <schema_username>
IDENTIFIED BY <schema_password>
DEFAULT TABLESPACE users
TEMPORARY TABLESPACE TEMP
QUOTA UNLIMITED ON users;
```

7. Grant the schema owner role to the user.

```
GRANT <schema_owner_role> to <schema_username>;
```

8. Create the data source user.

```
CREATE USER <data_source_username>
IDENTIFIED BY <data_source_password>
DEFAULT TABLESPACE users
TEMPORARY TABLESPACE TEMP
QUOTA UNLIMITED ON users;
```

9. Grant the data source role to the user.

```
GRANT <data_source_role> to <data_source_username>;
```

The installer grants the data source user access to the application database objects. If you choose **No** on the Manual Deployment Option screen, you need to grant the access after the installer completes. For more information, see ["Manual Deployment of the Returns Management Application"](#).

## Expand the Returns Management Distribution

To extract the Returns Management files:

1. Extract the ORRM-2.1.zip file from the Returns Management 2.1 distribution EPD zip file.
2. Log into the UNIX server as the user who owns the OracleAS 10g installation. Create a new staging directory for the Returns Management application distribution (ORRM-2.1.zip), for example, /tmp/j2ee/orrm-inst/orrm-staging.

---

**Note:** The staging directory (*staging\_directory*) can exist anywhere on the system. It does not need to be under ORACLE\_HOME.

---

3. Copy or upload ORRM-2.1.zip to *staging\_directory* and extract its contents. The following files and directories should be created under *staging\_directory/ORRM-2.1*:

```
ant/  
ant-ext/  
antinstall/  
returnsmgmt/  
connectors/  
external-lib/  
installer-resources/  
.postinstall.cmd  
.postinstall.sh  
.preinstall.cmd  
.preinstall.sh  
.preinstall-oas.cmd  
.preinstall-oas.sh  
.preinstall-was.cmd  
.preinstall-was.sh  
antinstall-config.xml  
build.xml  
build-common.xml  
build-common-oas.xml  
build-common-was.xml  
build-common-webapps.xml  
checkdeps.cmd  
checkdeps.sh  
install.cmd  
install.sh  
jmsconfiguration.dat  
prepare.xml  
retail-OCM.zip
```

For the remainder of this chapter, *staging\_directory/ORRM-2.1* is referred to as *<INSTALL\_DIR>*.

## Obtain Third-Party Library Files Required by Returns Management

The Returns Management application uses the Pager Tag Library from JSPTags. You must download the `pager-taglib.jar` file from the JSPTags website before running the Returns Management application installer.

1. Download the `pager-taglib-2.0.war` file from the JSPTags website:  
<http://jsptags.com/tags/navigation/pager/download.jsp>
2. Extract the `pager-taglib.jar` file from the `WEB-INF/lib` subdirectory in the `pager-taglib-2.0.war` file. Copy `pager-taglib.jar` into *<INSTALL\_DIR>/external-lib/*.

## Installation Options

During installation, there are options that enable you to select whether the installer completes parts of the installation or if you want to complete those parts manually. For information on the available options, see the following sections:

- ["Database Install Options"](#)
- ["Manual Deployment of the Returns Management Application"](#)
- ["Install Parameters Option"](#)

For information on manually deploying the Key Store, see ["Manual Deployment of the Key Store"](#).

## Database Install Options

The database schema must be created and populated before configuring the application server. On the Database Install Options screen, you select whether the installer creates and populates the database schema and seed data or if you want to do this manually.

- If you choose Yes, you do not need to perform any further steps. The installer will create and populate the database. This is the default selection on the screen.
- If you choose No, the installer does not create and populate the database schema.

---



---

**Note:** You must populate the database schema before running the installer. Otherwise, the installer will fail when configuring security.

---



---

To create and populate the database schema:

1. Change to the `<INSTALL_DIR>/centraloffice/db` directory.
2. Set the `JAVA_HOME` and `ANT_HOME` environment variables. You can use the JDK and Ant that are installed with the Oracle Application Server.

```
JAVA_HOME=$ORACLE_HOME/jdk; ANT_HOME=<INSTALL_DIR>/ant; export JAVA_HOME ANT_HOME
```

3. Add `$JAVA_HOME/bin` and `$ANT_HOME/bin` to the front of the `PATH` environment variable.

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:$PATH; export PATH
```

4. Expand the `centralofficeDBInstall.jar` file.

```
jar -xvf centralofficeDBInstall.jar
```

5. Modify `db.properties`.

- a. Uncomment the Oracle properties and comment out the properties for the other vendors such as DB2 and MS-SqlServer.
- b. Set the following properties with your database settings. The values to be set are shown in bold in the examples.

Set the hash algorithm, for example, to SHA-256.

```
# Hash Algorithm
inst.hash.algorithm=HASH_ALGORITHM
```

Enter the values for the users shown in bold in the following example:

```
inst.app.admin.user=my-pos-admin-user
inst.app.admin.password-encrypted=my-encrypted-pos-admin-password
```

```
db.user=DB_USER_ID
db.password-encrypted=DB_PASSWORD_ENCRYPTED
```

```
db.owner.user=DB_OWNER_USER_ID
db.owner.password-encrypted=DB_OWNER_PASSWORD_ENCRYPTED
```

The ant target will prompt for the passwords. Run the following ant target to encrypt the passwords:

```
ant -f db.xml encrypt-webapp-passwords
```

Enter the values for the URL used by the Returns Management application to access the database schema. See [Appendix E](#) for the expected syntax:

```
db.jdbc-url=jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME
```

- c. Set the `ora.home.dir` property to point to your Oracle Application Server installation.
  - d. Set the host name and port number for the `parameter.apphost` property to point to your Central Office installation.
  - e. In the `parameters.classpath` property, replace the semicolons used as separators with colons. This is needed to run with UNIX systems.
6. Uncomment the following properties in `jndi.properties`. This file is in the `jndi` directory.

```
java.naming.factory.initial=com.evermind.server.rmi.RMIInitialContextFactory
java.naming.security.principal=<user>
java.naming.security.credentials=<user>
```

7. Run one of the available Ant targets to create the database schema and load data:
  - a. `load_sql`: creates tables and other objects; calls `seed_data`
  - b. `seed_data`: loads seed data

For example, `ant load_sql`

## Secure the JDBC for the Oracle 11g Database

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. See [Figure A-6](#) in [Appendix A](#).

- If **Yes** is selected, the installer sets up the secure JDBC.
- If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see [Appendix I](#).



## Install the Java Cryptography Extension (JCE)

If you are using the RSA Key Manager, you must update the security for your JRE. You need to obtain version 5.0 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

1. Make a backup copy of `local_policy.jar` and `US_export_policy.jar`.

```
cd $ORACLE_HOME/jdk/jre/lib/security
mv local_policy.jar local_policy.jar.bak
mv US_export_policy.jar US_export_policy.jar.bak
```

2. Download version 5.0 of the JCE.

- a. Go to the following website:

[http://java.sun.com/javase/downloads/index\\_jdk5.jsp](http://java.sun.com/javase/downloads/index_jdk5.jsp)

- b. Under Other Downloads, find **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0**.

- c. Click **Download**.

- d. Follow the instructions to download the JCE.

3. Copy the jar files into the JRE security directory. The files are bundled as `jce_policy-1_5_0.zip`.

## Run the Returns Management Application Installer

Once you have an OC4J instance that is configured and started, you can run the Returns Management application installer. This installer will configure and deploy the Returns Management application.

---

---

**Note:** To see details on every screen and field in the application installer, see [Appendix A](#).

---

---

1. Change to the `<INSTALL_DIR>` directory.
2. Set the `ORACLE_HOME` and `JAVA_HOME` environment variables.

`ORACLE_HOME` should point to your OracleAS 10g installation, for example, `/opt/Oracle/10.1.3.4/OracleAS_1`.

`JAVA_HOME` should point to `%ORACLE_HOME%/jdk`.

---

---

**Note:** The installer is not compatible with versions of Java earlier than 1.5.

---

---

3. If you are using an X server such as Exceed, set the `DISPLAY` environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset `DISPLAY` for text mode or use the `install.sh` script.

---

---

**Caution:** Password fields are masked in GUI mode, but in text mode your input is shown in plain text in the console window.

---

---

4. Run the installer.
  - a. Log into the UNIX server as the user who owns the OracleAS 10g installation.
  - b. Change the mode of all .sh files to executable.
  - c. Run the install.sh script. This will launch the installer.

---

**Note:** The usage details for install.sh are shown below. The typical usage for GUI mode does not use arguments.

```
install.sh [text | silent oracle]
```

---

After installation is complete, a detailed installation log file is created:  
/orm-install-app.<timestamp>.log

5. The installer leaves behind the /ant.install.properties file for future reference and repeat installations. This file contains all the inputs you provided, including passwords. As a security precaution, make sure that the file has restrictive permissions.

```
chmod 600 ant.install.properties
```

6. Verify that the installer was able to delete the \$ORACLE\_HOME/jdk/jre/lib/ext/security-360-ora.jar file. This is a file that is temporarily created by the installer. If the installer was unable to delete the file, you must shut down all OC4J instances, delete the file manually, and start the OC4J instances back up again.

---

**Note:** If the installer is unable to delete this file, it prints a warning that instructs you to delete it manually. This warning also shows up at the end of the installer log file.

---

## Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, it will halt execution immediately. You can run the installer in silent mode so that you do not have to reenter the settings for your environment. For instructions on silent mode, see [Appendix C](#).

For a list of common installation errors, see [Appendix F](#).

Since the application installation is a full reinstall every time, any previous partial installs will be overwritten by the successful installation.

## Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM.

The following document is available through My Oracle Support (formerly MetaLink). Access My Oracle Support at the following URL:

<https://metalink.oracle.com>

***Oracle Configuration Manager Installer Guide (Doc ID: 835024.1)***

This guide describes the procedures and interface of the Oracle Retail Oracle Configuration Manager Installer that a retailer runs near the completion of its installation process.

**OCM Documentation Link**

<http://www.oracle.com/technology/documentation/ocm.html>

## Backups Created by Installer

The Oracle Retail Returns Management application installer will back up modified application server files and directories by renaming them with a timestamp. This is done to prevent the removal of any custom changes you might have. These backup files and directories can be safely removed without affecting the current installation. For example, the file could be named `jms.xml.200711011326`.

## Manual Deployment of the Key Store

If you implement a Key Store interface, you can use the rar file to manually deploy the Key Store on the application server.

- To deploy using an ant target:

1. Copy the following properties into the `ant.install.properties` file:

```
## Properties from Page:InternalDeployKeyStoreRAR
input.internal.keystore.rar.deploy.enabled = true
input.internal.keystore.rar.deploy.name = keystoreconnector
input.internal.keystore.rar.deploy.file = <INSTALL_DIR>/connectors/
sim-keystoreconnector-rar.rar
```

2. Run the following ant target:

```
install.sh ant init keystore-rar-deploy -propertyfile
ant.install.properties
```

- To deploy from the application server console, log in to the application server console and deploy the rar file. The rar file is located at:

```
<INSTALL_DIR>/connectors/sim-keystoreconnector-rar.rar
```

## Install Parameters Option

The application parameters must be installed before the Returns Management application is fully operational. On the Install Parameters screen, you select whether the installer completes installation of the parameters or if you want to do this manually.

- If you chose Yes, you do not need to perform any further steps to install the parameters. This is the default selection on the screen.
- If you chose No, the installer did not install the parameters. For information on installing the parameters, see ["Import Initial Parameters"](#).

## Manual Deployment of the Returns Management Application

Skip this section if you chose the default option of allowing the installer to complete installation to the application server.

The installer includes the option to configure the application locally and skip deployment to the application server. If this option is chosen, the installer will make the configured application files available under

`<INSTALL_DIR>/returnsmgmt/configured-output/`.

If you chose this installer option, you can deploy the Returns Management ear file by following these steps:

- To deploy using the ant target:
  1. Check that the Key Store JNDI name in the `<orbo-inst>/applib/spring.properties` file matches the JNDI name of the Key Store deployed on the application server.
  2. Update the following property in the `ant.install.properties` file.

```
input.install.to.appserver = true
```

3. Run the following ant target:

```
install.sh ant init app-ear-deploy -propertyfile ant.install.properties
```

- To deploy from the application server console, log in to the application server console and deploy the ear file. The ear file is located at:

```
<INSTALL_DIR>/returnsmgmt/configured-output
```

When deploying the ear file, you should provide the same application name and context root you gave to the installer. These values were stored in the

`<INSTALL_DIR>/ant.install.properties` file by the installer for later reference.

## Import Initial Parameters

---

**Note:** An initial set of parameters must be imported before you can use Oracle Retail Returns Management. For more information on parameters, see the *Oracle Retail Strategic Store Solutions Configuration Guide*.

---

This section provides an overview of the procedures for importing an initial set of parameters. You can import the parameters through the Oracle Retail Returns Management user interface or by using an ant target. You only need to use one of the procedures. The procedure for importing parameters through the application user interface is described in more detail in the *Oracle Retail Returns Management User Guide*.

These instructions assume you have already expanded the `returnsmgmtDBInstall.jar` file under the `<INSTALL_DIR>` directory as part of the database schema installation earlier in this chapter.

### Importing Parameters Through the User Interface

To import the initial parameters through the user interface:

1. Open the Oracle Retail Returns Management application in a web browser. The address is provided at the end of the installer output and in the log file.  
`http://<servername>:<portnumber>/<context root>`
2. Log in to the application as user ID **pos** and password **pos**, or any other user ID that has full administrative rights.
3. Click the **Data Management** tab. The Available Imports screen appears.
4. To import the master parameter set, click the **File** link in the Import Parameters for Distribution row. Follow the instructions to import `parameterset.xml` from the `<INSTALL_DIR>/returnsmgmt/db` folder.
5. To import the initial set of Oracle Retail Returns Management application parameters, click the **File** link in the Import Application Parameters row. Follow the instructions to import `returnsmgmt.xml` from the `<INSTALL_DIR>/returnsmgmt/db` folder.

### Importing Parameters By Using an Ant Target

To import parameters using an ant target:

1. Change to the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
2. Edit the `db.properties` file. Update the following properties in the "Properties for Parameter Loading" section.
  - a. Change `ora.home.dir` to your Oracle Application Server installation directory, for example:  
`ora.home.dir=/opt/Oracle/10.1.3.4/OracleAS_1`
  - b. Change `<ORA_HOST_NAME>` to your host name, `<port number>` to your RMI port number, and `<application name>` to your application name.  
`parameters.apphost=ormi://<ORA_HOST_NAME>:<port number>/<application name>`

3. Run the following command:

```
ant load_parameters
```

## Load Optional Purge Procedures

For information on how to invoke the procedures provided for purging aged data, see the *Oracle Retail Returns Management Operations Guide*.

To load the purge procedures:

1. Run the available Ant target to load the procedures.

```
ant load_purge_procedures
```

2. Log in as the database schema owner, *<schema\_username>*.
3. Create a user for running the purge procedures. This user should only have the privileges required to run the purge procedures.

## Using the Returns Management Application

---

---

**Note:** When you are done installing Returns Management, log out and close the browser window. This ensures that your session information is cleared and prevents another user from accessing Returns Management with your login information.

---

---

After the application installer completes and you have run the initial parameter load, you should have a working Returns Management application installation. To launch the application, open a web browser and go to

`https://<servername>:<portnumber>/<context root>`

For example, `https://myhost:443/returnsmanagement`

---

## Installation of the IBM Stack on IRES

Before proceeding, you must install the database, create the database schema, and install the application server software. For a list of supported versions, see [Chapter 1](#).

During installation, the Returns Management database schema will be created and the Returns Management application will be deployed. The Java JDK that is included with the IBM WebSphere Application Server will be used to run the application.

### Check the WebSphere Application Server Settings

Some application server settings affect Returns Management processing and deployment. Verify that these settings are set correctly for your installation.

### Authentication Cache Timeout

The Authentication Cache Timeout setting for the IBM WebSphere application server must be set correctly for Returns Management password processing. For information on how to determine the value you should use for this setting and how to set the value for the application server, refer to your IBM WebSphere documentation.

### Create the Database Schema Owner and Data Source Users

The following recommendations should be considered for schema owners:

- Database administrators should create an individual schema owner for each application, unless the applications share the same data. In the case of Oracle Retail Back Office and Point-of-Service, the database schema owner are the same because these applications share a database.
- The schema owners should only have enough privileges to install the database.

For information on best practices for passwords, see [Appendix H](#).

To create the database schema owner and data source users:

1. Log in using the database administrator user ID.
2. Create the schema owner user.

```
CREATE SCHEMA <schema_name> AUTHORIZATION <schema_username>
```

3. Grant the privileges, shown in the following example, to the user.

```
GRANT CREATETAB, BINDADD, CONNECT, IMPLICIT_SCHEMA ON DATABASE TO USER  
<schema_username>
```

4. Grant the following object level privileges to the schema owner user.

```
GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA <schema_name> TO USER  
<schema_username> WITH GRANT OPTION
```

5. Create the data source user.

```
CREATE SCHEMA <data_source_schema_name> AUTHORIZATION <data_source_username>
```

6. Grant the privileges, shown in the following example, to the data source user.

```
GRANT CONNECT, IMPLICIT_SCHEMA ON DATABASE TO USER <data_source_username>
```

7. Grant the following object level privileges to the data source user.

```
GRANT CREATEIN ON SCHEMA <data_source_schema_name> TO USER <data_source_<br/>username> WITH GRANT OPTION
```

The installer grants the data source user access to the application database objects. If you choose **No** on the Manual Deployment Option screen, you need to grant the access after the installer completes. For more information, see ["Manual Deployment of the Returns Management Application"](#).

## Expand the Returns Management Distribution

To extract the Returns Management files:

1. Extract the ORRM-2.1.zip file from the Returns Management 2.1 distribution EPD zip file.
2. Log in to the UNIX server as the user who owns the WebSphere AS installation. Create a new staging directory for the Returns Management application distribution (ORRM-2.1.zip), for example, /tmp/orrm-staging.

---

---

**Note:** The staging directory (<staging\_directory>) can exist anywhere on the system. It does not need to be under tmp.

---

---

3. Copy or upload ORRM-2.1.zip to the staging directory and extract its contents. The following files and directories should be created under <staging\_directory>/ORRM-2.1:

```
ant/  
ant-ext/  
antinstall/  
returnsmgmt/  
connectors/  
external-lib/  
installer-resources/  
.postinstall.cmd  
.postinstall.sh  
.preinstall.cmd  
.preinstall.sh  
.preinstall-oas.cmd  
.preinstall-oas.sh  
.preinstall-was.cmd  
.preinstall-was.sh  
antinstall-config.xml  
build.xml  
build-common.xml  
build-common-oas.xml
```



```

build-common-was.xml
build-common-webapps.xml
checkdeps.cmd
checkdeps.sh
install.cmd
install.sh
jmsconfiguration.dat
prepare.xml
retail-OCM.zip

```

For the remainder of this chapter, *<staging\_directory>/ORRM-2.1* is referred to as *<INSTALL\_DIR>*.

## Obtain Third-Party Library Files Required by Returns Management

The Returns Management application uses the Pager Tag Library from JSPTags and the DB2 drivers from IBM. Before running the Returns Management application installer, you must download the necessary files from the JSPTags website and the IBM website.

1. Download the `pager-taglib-2.0.war` file from the JSPTags website:  
<http://jsptags.com/tags/navigation/pager/download.jsp>
2. Extract the `pager-taglib.jar` file from the `WEB-INF/lib` subdirectory in the `pager-taglib-2.0.war` file. Copy `pager-taglib.jar` into *<INSTALL\_DIR>/external-lib/*.
3. Download the `db2_db2driver_for_jdbc_sqlj.zip` file from the IBM website:  
<http://www.ibm.com/software/data/db2/java/>  
You need an IBM ID, which you can request from the Sign in screen, in order to log in to this website.
4. Extract the `db2jcc.jar` file from the `db2_db2driver_for_jdbc_sqlj` directory in the `db2_db2driver_for_jdbc_sqlj.zip` file. Copy `db2jcc.jar` into *<INSTALL\_DIR>/external-lib/*.
5. Obtain the `db2jcc_license_cu.jar` file from your database server. Copy `db2jcc_license_cu.jar` into *<INSTALL\_DIR>/external-lib/*.

---

**Note:** The `db2jcc_license_cu.jar` file is needed to permit JDBC/SQLJ connectivity to the IBM DB2 database. The file is the standard license included with all editions of the IBM DB2 database.

---

## Securing the JDBC for the IBM DB2 Database

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. See [Figure B-6](#) in [Appendix B](#).

- If **Yes** is selected, you must install the database digital certificate into the application server truststore.
  1. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  2. Expand the Security menu.
  3. Click the **SSL certificate and key management** option.
  4. In the Related Items list, click **Key stores and certificates**.
  5. Click the **NodeDefaultTrustStore** link in the list.

6. In the Additional Properties list, click the **Signer certificates** link.
  7. Click the **Add** button.
  8. Enter a distinct alias and the full path to the certificate file on the server in the File name field. Make sure the Data type corresponds to the type in the file. The certificate should appear in the list of Signer certificates.
- If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see [Appendix J](#).

## Install the Java Cryptography Extension (JCE)

If you are using RSA Key Manager, you must update the security for your JRE. You need to obtain version 1.4.2+ of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. The 1.4.2+ version for the JCE Unlimited Strength Encryption is compatible with the IBM Java5 JRE.

1. Make a backup copy of `local_policy.jar` and `US_export_policy.jar`.  

```
cd <WAS_INSTALL_DIR>/java/jre/lib/security
mv local_policy.jar local_policy.jar.bak
mv US_export_policy.jar US_export_policy.jar.bak
```
2. Download version 1.4.2+ of JCE.
  - a. Go to the following website:  
<http://www.ibm.com/developerworks/java/jdk/security/50/>
  - b. Click **IBM SDK Policy Files**. You are prompted to log in. You need an IBM ID, which you can request from the Sign in screen, in order to log in to this website.
  - c. After you log in, follow the instructions to download the JCE.
3. Copy the jar files into the JRE security directory. The files are bundled as `unrestricted.zip`.

## Installation Options

During installation, there are options that enable you to select whether the installer completes parts of the installation or if you want to complete those parts manually. For information on the available options, see the following sections:

- ["Database Install Options"](#)
- ["Configure IBM WebSphere MQ"](#)
- ["Manual Deployment of the Returns Management Application"](#)
- ["Install Parameters"](#)

For information on manually deploying the Key Store, see ["Manual Deployment of the Key Store"](#).

## Database Install Options

The database schema must be created and populated before configuring the application server. On the Database Install Options screen, you select whether the installer creates and populates the database schema and seed data or if you want to do this manually.

- If you choose Yes, you do not need to perform any further steps. The installer will create and populate the database. This is the default selection on the screen.
- If you choose No, the installer does not create and populate the database schema.

---

**Note:** You must populate the database schema before running the installer. Otherwise, the installer will fail when configuring security.

---

To create and populate the database schema:

1. Change to the `<INSTALL_DIR>/returnsmgmt/db` directory.
2. Set the `JAVA_HOME` and `ANT_HOME` environment variables. You can use the JDK and Ant that are installed with the IBM WebSphere Application Server.

```
JAVA_HOME=<WAS_INSTALL_DIR>/Java; ANT_HOME=<INSTALL_DIR>/ant;
export JAVA_HOME ANT_HOME
```

3. Add `$JAVA_HOME/bin` and `$ANT_HOME/bin` to the front of the `PATH` environment variable.

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:$PATH; export PATH
```

4. Expand the `returnsmgmtDBInstall.jar` file.

```
jar -xvf returnsmgmtDBInstall.jar
```

5. Modify `db.properties`.

- a. Uncomment the DB2 properties and comment out the properties for the other vendors such as Oracle and MS-SqlServer.
- b. Set the following properties with your database settings. The values to be set are shown in bold in the examples.

Set the hash algorithm, for example, to SHA-256.

```
# Hash Algorithm
inst.hash.algorithm=HASH_ALGORITHM
```

Enter the values for the users shown in bold in the following example:

```
inst.app.admin.user=my-pos-admin-user
inst.app.admin.password-encrypted=my-encrypted-pos-admin-password
```

```
db.user=DB_USER_ID
db.password-encrypted=**DB_PASSWORD_ENCRYPTED**
```

```
db.owner.user=DB_OWNER_USER_ID
db.owner.password-encrypted=**DB_OWNER_PASSWORD_ENCRYPTED**
```

The ant target will prompt for the passwords. Run the following ant target to encrypt the passwords:

```
ant -f db.xml encrypt-webapp-passwords
```

Enter the values for the URL used by the Returns Management application to access the database schema. See [Appendix E](#) for the expected syntax:

```
db.jdbc-url=jdbc:db2://DB_HOST_NAME:50001/DB_NAME
```

- c. Set the `was.home.dir` property to point to your IBM WebSphere Application Server installation.
  - d. Set the host name and port number for the `parameter.apphost` property to point to your Returns Management installation.
  - e. In the `parameters.classpath` property, replace the semicolons used as separators with colons. This is needed to run with UNIX systems.
6. Uncomment the following properties in `jndi.properties`. This file is in the `jndi` directory.

```
java.naming.factory.initial=com.evermind.server.rmi.RMIInitialContextFactory
java.naming.security.principal=<user>
java.naming.security.credentials=<user>
```

7. Run one of the available Ant targets to create the database schema and load data:
- a. `load_sql`: creates tables and other objects; calls `seed_data`
  - b. `seed_data`: loads seed data

For example, `ant load_sql`

## Run the Returns Management Application Installer

The installer will configure and deploy the Returns Management application. Before running the installer, verify that a profile has been created and the IBM WebSphere application server is running.

---

---

**Note:** To see details on every screen and field in the application installer, see [Appendix B](#).

---

---

1. Change to the `<INSTALL_DIR>` directory.
2. Set the `JAVA_HOME` environment variable to point to the Java in the IBM WebSphere application server, that is, `<WAS_INSTALL_DIR>/Java`.

---

---

**Note:** The installer is not compatible with versions of Java earlier than 1.5.

---

---

3. If you are using an X server such as Xceed, set the `DISPLAY` environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset `DISPLAY` for text mode or use the `install.sh` script.

---

---

**Caution:** Password fields are masked in GUI mode, but in text mode your input is shown in plain text in the console window.

---

---

4. Run the installer.
  - a. Log into the UNIX server as a user who is authorized to install software.
  - b. Change the mode of all .sh files to executable.
  - c. Run the `install.sh` script. This will launch the installer.

---

**Note:** The usage details for `install.sh` are shown below. The typical usage for GUI mode does not use arguments.

---

```
install.sh [text | silent webspere]
```

---

After installation is complete, a detailed installation log file is created:  
`/orrm-install-app.<timestamp>.log`

5. The installer leaves behind the `/ant.install.properties` file for future reference and repeat installations. This file contains all the inputs you provided, including passwords. As a security precaution, make sure that the file has restrictive permissions.

```
chmod 600 ant.install.properties
```

## Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, it will halt execution immediately. You can run the installer in silent mode so that you do not have to reenter the settings for your environment. For instructions on silent mode, see [Appendix C](#).

For a list of common installation errors, see [Appendix F](#).

Since the application installation is a full reinstall every time, any previous partial installs will be overwritten by the successful installation.

## Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM.

The following document is available through My Oracle Support (formerly MetaLink). Access My Oracle Support at the following URL:

<https://metalink.oracle.com>

### *Oracle Configuration Manager Installer Guide (Doc ID: 835024.1)*

This guide describes the procedures and interface of the Oracle Retail Oracle Configuration Manager Installer that a retailer runs near the completion of its installation process.

### **OCM Documentation Link**

<http://www.oracle.com/technology/documentation/ocm.html>

## Manual Deployment of the Key Store

If you implement a Key Store interface, you can use the rar file to manually deploy the Key Store on the application server.

- To deploy using an ant target:

1. Copy the following properties into the `ant.install.properties` file:

```
## Properties from Page:InternalDeployKeyStoreRAR
input.internal.keystore.rar.deploy.enabled = true
input.internal.keystore.rar.deploy.name = keystoreconnector
input.internal.keystore.rar.deploy.file = <INSTALL_DIR>/connectors/
sim-keystoreconnector-rar.rar
```

2. Run the following ant target:

```
install.sh ant init keystore-rar-deploy -propertyfile
ant.install.properties
```

- To deploy from the application server console, log in to the application server console and deploy the rar file. The rar file is located at:

```
<INSTALL_DIR>/connectors/sim-keystoreconnector-rar.rar
```

## Configure IBM WebSphere MQ

IBM WebSphere MQ, formerly known as IBM MQ Series, must be configured with a queue manager and the JMS queues and topics required by Returns Management, before Returns Management can be deployed. On the Configure MQ Series Option screen, you select whether the installer configures IBM WebSphere MQ or if you manually configure it.

---

---

**Note:** If IBM WebSphere MQ is installed on a different machine than IBM WebSphere Application Server, you must manually configure it.

---

---

Typically, when IBM WebSphere MQ is installed, a special user ID (usually `mqm`), and a user group (also `mqm`) are created in the operating system. The MQ installation files and directories have their owner and group set to the IBM WebSphere MQ user ID and group ID.

The user ID used for the Returns Management installation, must be made a member of IBM WebSphere MQ's user group, before attempting to create the Returns Management queue manager, queues, and topics. For example, if Returns Management is installed as user `root`, then `root` must be made a member of the `mqm` group.

Use the following commands to configure IBM WebSphere MQ. `MQ_Install_Dir` is the directory where IBM WebSphere MQ was installed. The values for `<input.jms.server.queue>` and `<input.jms.server.port>` come from the `ant.install.properties` file.

```
<MQ_Install_Dir>/bin/crtmqm -q <input.jms.server.queue>
<MQ_Install_Dir>/bin/strmqm <input.jms.server.queue>
<MQ_Install_Dir>/bin/runmqslr -m <input.jms.server.queue> -p
<input.jms.server.port> -t tcp &
<MQ_Install_Dir>/bin/runmqsc <input.jms.server.queue> <
<INSTALL_DIR>/returnsmgmt/appserver/was/createq.dat

<MQ_Install_Dir>/bin/runmqsc <input.jms.server.queue> <
<MQ_Install_Dir>/java/bin/MQJMS_PSQ.mqsc
<MQ_Install_Dir>/bin/strmqbrk -m <input.jms.server.queue>
```

## Manual Deployment of the Returns Management Application

Skip this section if you chose the default option of allowing the installer to complete installation to the application server.

The installer includes the option to configure the application locally and skip deployment to the application server. If this option is chosen, the installer will make the configured application files available under `<INSTALL_DIR>/returnsmgmt/configured-output/`.

If you chose this installer option, you can deploy the Returns Management ear file by following these steps:

- To deploy using the ant target:
  1. Check that the Key Store JNDI name in the `<orbo-inst>/applib/spring.properties` file matches the JNDI name of the Key Store deployed on the application server.
  2. Update the following property in the `ant.install.properties` file.
 

```
input.install.to.appserver = true
```
  3. Run the following ant target:
- To deploy from the application server console, log in to the application server console and deploy the ear file. The ear file is located at:

```
<INSTALL_DIR>/returnsmgmt/configured-output
```

When deploying the ear file, you should provide the same application name and context root you gave to the installer. These values were stored in the `<INSTALL_DIR>/ant.install.properties` file by the installer for later reference.

## Install Parameters

The application parameters must be installed before the Returns Management application is fully operational. On the Install Parameters screen, you select whether the installer completes installation of the parameters or if you want to do this manually.

- If you chose Yes, you do not need to perform any further steps to install the parameters. This is the default selection on the screen.
- If you chose No, the installer did not install the parameters. For information on installing the parameters, see ["Import Initial Parameters"](#).

## Import Initial Parameters

---

---

**Note:** If you did not choose to have the installer set the initial parameters, you must import an initial set of parameters before you can use Returns Management. For more information on parameters, see the *Oracle Retail Strategic Store Solutions Configuration Guide*.

---

---

This section provides an overview of the procedures for importing an initial set of parameters. You can import the parameters through the Returns Management user interface or by using an Ant target. You only need to use one of the procedures. The procedure for importing parameters through the application user interface is described in more detail in the *Oracle Retail Returns Management User Guide*.

These instructions assume you have already expanded the `centralofficeDBInstall.jar` file under the `<INSTALL_DIR>` directory as part of the database schema installation earlier in this chapter.

## Importing Parameters Through the User Interface

To import the initial parameters through the user interface:

1. Open the Returns Management application in a web browser. The address is provided at the end of the installer output and in the log file.  
`http://<your host name>:<your port number>/<context root>`
2. Log in to the application with a user ID that has full administrative rights.
3. Click the **Data Management** tab. The Available Imports screen appears.
4. To import the master parameter set, click the **File** link in the Import Parameters for Distribution row. Follow the instructions to import `parameterset.xml` from the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
5. To import the initial set of Returns Management application parameters, click the **File** link in the Import Application Parameters row. Follow the instructions to import `returnsmgmt.xml` from the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.



## Importing Parameters By Using an Ant Target

To import parameters using an Ant target:

1. Change to the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
2. Execute the following command:

```
ws_ant load_parameters
```

## Load Optional Purge Procedures

For information on how to invoke the procedures provided for purging aged data, see the *Oracle Retail Returns Management Operations Guide*.

To load the purge procedures:

1. Run the available Ant target to load the procedures.  

```
ant load_purge_procedures
```
2. Log in as the database schema owner, `<schema_username>`.
3. Create a user for running the purge procedures. This user should only have the privileges required to run the purge procedures.

## Using the Returns Management Application

---

---

**Note:** When you are done installing Returns Management, log out and close the browser window. This ensures that your session information is cleared and prevents another user from accessing Returns Management with your login information.

---

---

After the application installer completes and you have run the initial parameter load, you should have a working Returns Management application installation. To launch the application, open a web browser and go to

```
https://<servername>:<portnumber>/<context root>
```

For example, `https://myhost:9443/returnsmanagement`

---

---

**Note:** The installer created and started the MQ queue manager. If you restart WebSphere, you must also restart the MQ queue manager.

---

---



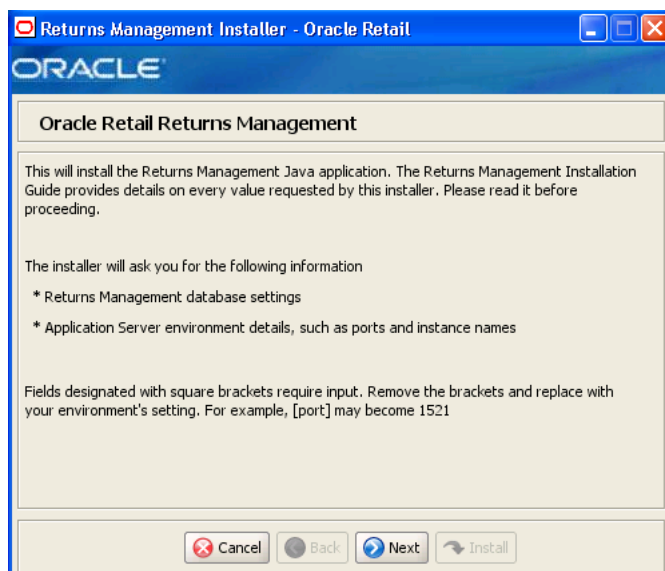
---

## Appendix: Returns Management Application Installer Screens for the Oracle Stack

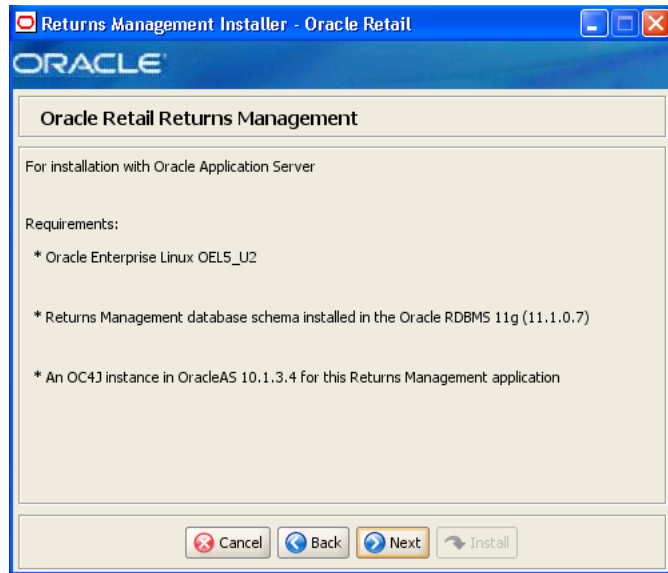
You need the following details about your environment for the installer to successfully deploy the Returns Management application on the Oracle stack. Depending on the options you select, you may not see some screens or fields.

For each field on a screen, a table is included in this appendix that describes the field. If you want to document any specific information about your environment for any field, a Notes row is provided in each table for saving that information.

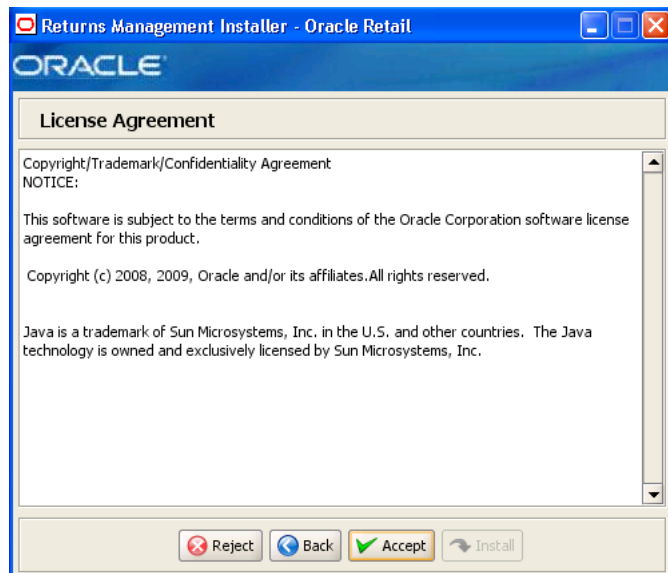
**Figure A-1** Introduction



**Figure A–2 Requirements**



**Figure A–3 License Agreement**



---

**Note:** You must choose to accept the terms of the license agreement in order for the installation to continue.

---

Figure A-4 Database Owner

Returns Management Installer - Oracle Retail

ORACLE

**Database Owner**

Provide the details for the Returns Management schema user that will create the schema objects.

Schema Username

Schema Password

Cancel Back Next Install

The fields on this screen are described in the following tables.

Field Title	Schema Username
Field Description	Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see <a href="#">"Create the Database Schema Owner and Data Source Users"</a> in <a href="#">Chapter 2</a> .  <b>Note:</b> This user creates the database objects used by Returns Management.
Example	DBOWNER
Notes	

Field Title	Schema Password
Field Description	Password for the database owner.
Notes	

**Figure A–5 Data Source User**

Returns Management Installer - Oracle Retail

ORACLE

**Data Source User**

Provide the details for the Returns Management schema user

JDBC URL

Data Source Username

Data Source password

Cancel Back Next Install

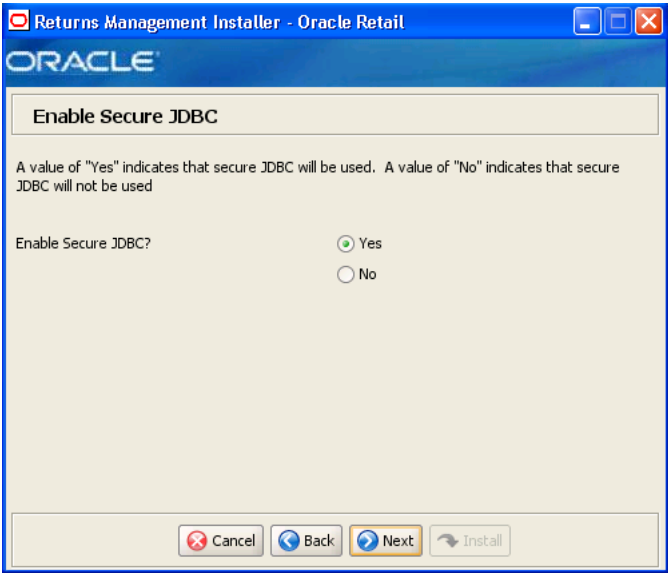
The fields on this screen are described in the following tables.

Field Title	JDBC URL
Field Description	URL used by the Returns Management application to access the database schema. See <a href="#">Appendix E</a> for the expected syntax.
Example	jdbc:oracle:thin:@myhost:1521:mydatabase
Notes	

Field Title	Data Source Username
Field Description	Database user name that can access and manipulate the data in the schema. This user can have Select, Insert, Update, Delete, and Execute privileges on objects in the schema, that is, Data Manipulation Language (DML) execution privileges. For information on creating this user, see " <a href="#">Create the Database Schema Owner and Data Source Users</a> " in <a href="#">Chapter 2</a> .
	<b>Note:</b> This schema user is used by Returns Management to access the database.
Example	DBUSER
Notes	

Field Title	Data Source Password
Field Description	Password for the data source user.
Notes	

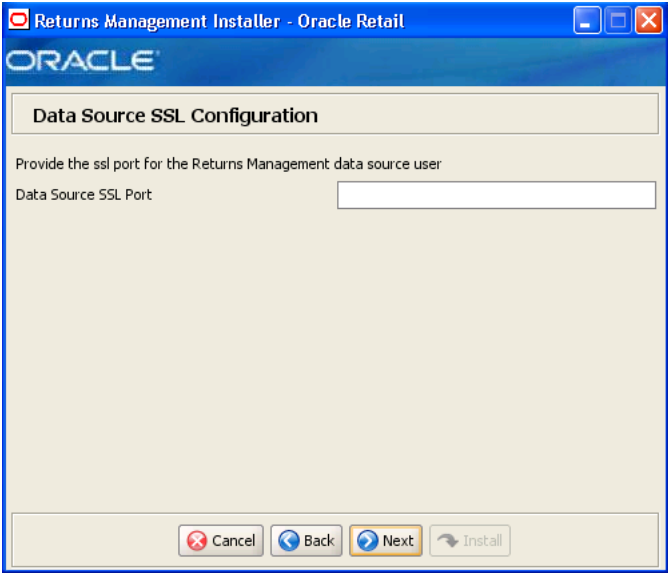
**Figure A–6 Enable Secure JDBC**



The field on this screen is described in the following table.

Field Title	Enable Secure JDBC?
Field Description	Select whether secure JDBC is to be used for communication with the database.
Example	Yes
Notes	

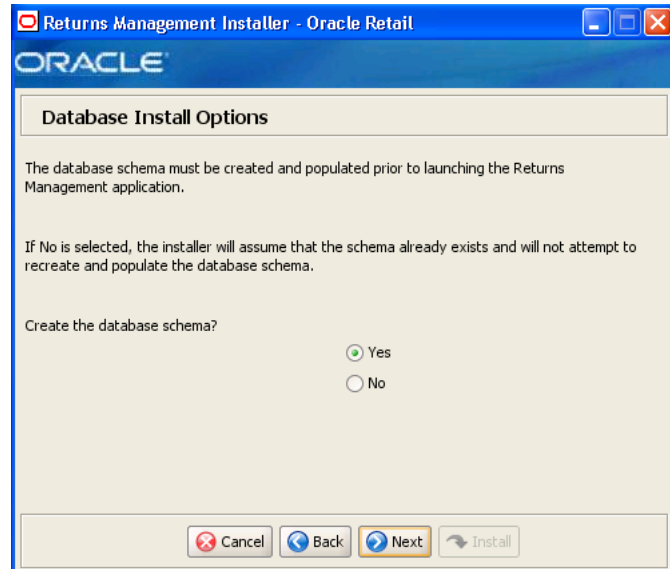
**Figure A–7 Data Source SSL Configuration**



This screen is only displayed if **Yes** is selected on the Enable Secure JDBC screen. The field on this screen is described in the following table.

Field Title	Data Source SSL Port
Field Description	SSL port used to access the database.
Example	1521
Notes	

**Figure A–8 Database Install Options**

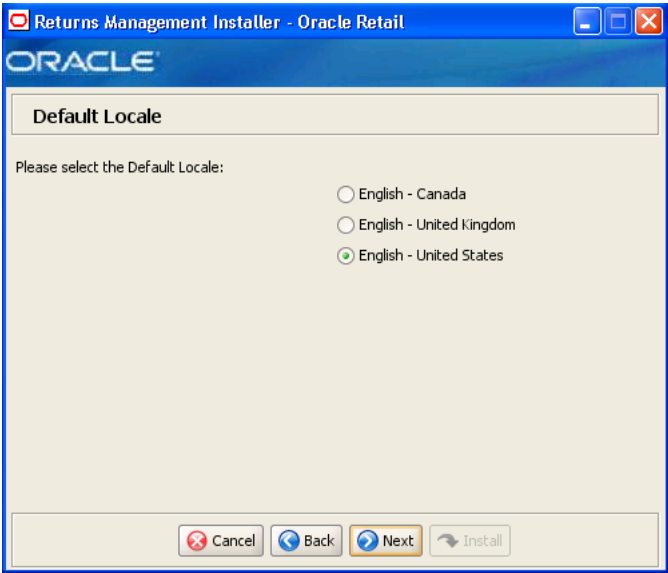


The field on this screen is described in the following table.

Field Title	Create database schema?
Field Description	<p>The database schema must be created and populated before starting Central Office. This screen gives you the option to have the installer create and populate the database schema or leave the database schema unmodified.</p> <ul style="list-style-type: none"> <li>■ To have the installer create and populate the database schema, select <b>Yes</b>.</li> <li>■ To have the installer leave the database schema unchanged, select <b>No</b>.</li> </ul> <p>For more information, see "<a href="#">Database Install Options</a>" in <a href="#">Chapter 2</a>.</p>
Example	Yes
Notes	



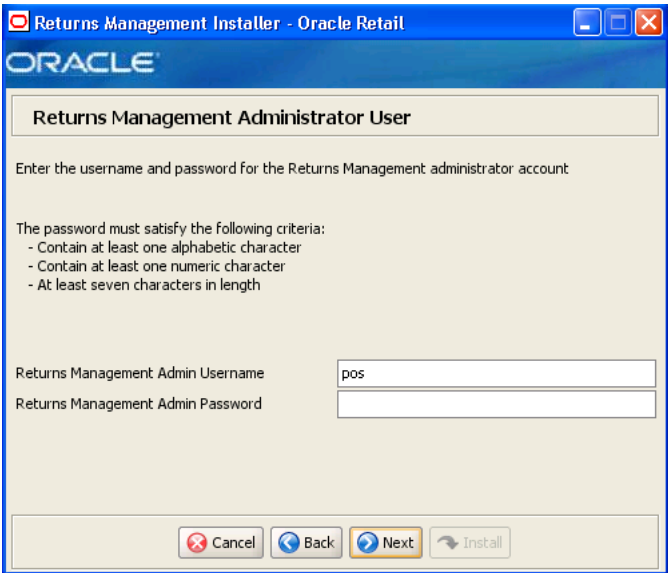
Figure A–9 Default Locale



The field on this screen is described in the following table.

Field Title	Please select the Default Locale
Field Description	Limited locale support in Returns Management enables the date, time, currency, and calendar to be displayed in the format for the selected default locale.  <b>Note:</b> The only language currently supported is United States English.
Example	English - United States
Notes	

Figure A–10 Returns Management Administrator User

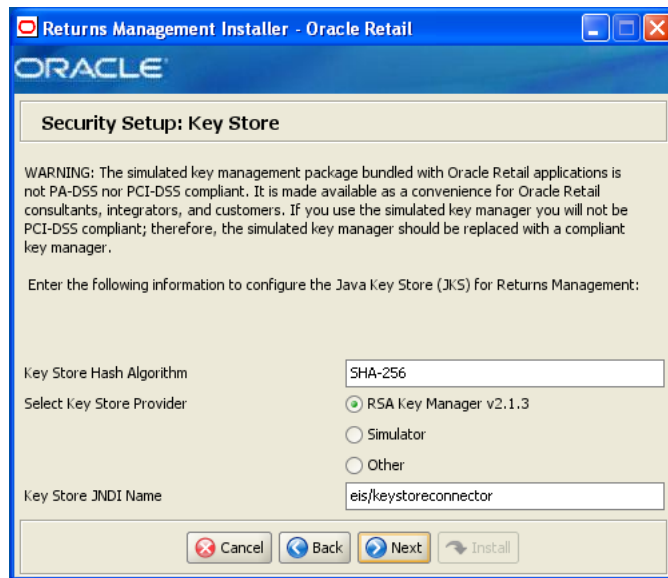


The fields on this screen are described in the following tables.

Field Title	Returns Management Administrator Username
Field Description	User name used for performing Returns Management administrative functions.
Example	pos
Notes	

Field Title	Returns Management Administrator Password
Field Description	Password for the administrator user.
Notes	

**Figure A–11 Security Setup: Key Store**



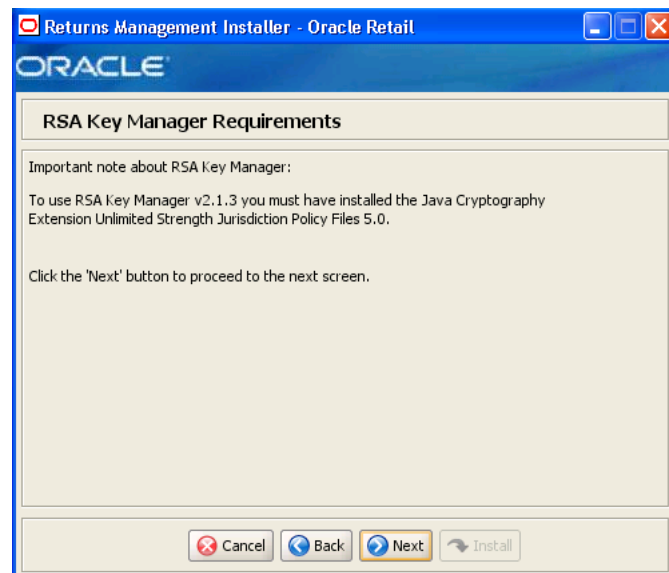
The fields on this screen are described in the following tables.

Field Title	Key Store Hash Algorithm
Field Description	Name of the algorithm used by the Key Store to hash sensitive data.
Example	SHA-256
Notes	

Field Title	Select Key Store Provider
Field Description	<p>Provider for Key Store management.</p> <ul style="list-style-type: none"> <li>To use the RSA key management package, select <b>RSA Key Manager v2.1.3</b>. The next screen displayed is <a href="#">Figure A-12</a>.</li> <li>To use the simulated key management package, select <b>Simulator</b>. The next screen displayed is <a href="#">Figure A-15</a>.</li> <li>To use a different key management provider, select <b>Other</b>. The next screen displayed is <a href="#">Figure A-16</a>.</li> </ul>
Example	RSA Key Manager v2.1.3
Notes	

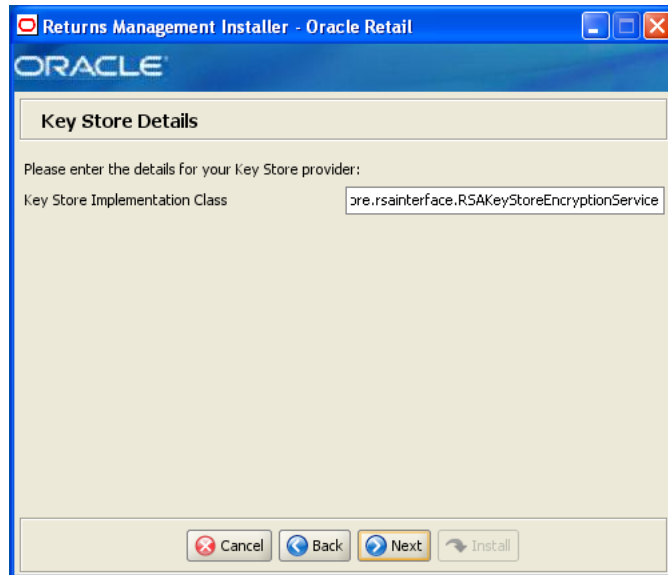
Field Title	Key Store JNDI Name
Field Description	Name of the Key Store JNDI.
Example	eis/keystoreconnector
Notes	

**Figure A-12 RSA Key Manager Requirements**



This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

**Figure A–13 Key Store Details for RSA Key Manager 2.1.3**

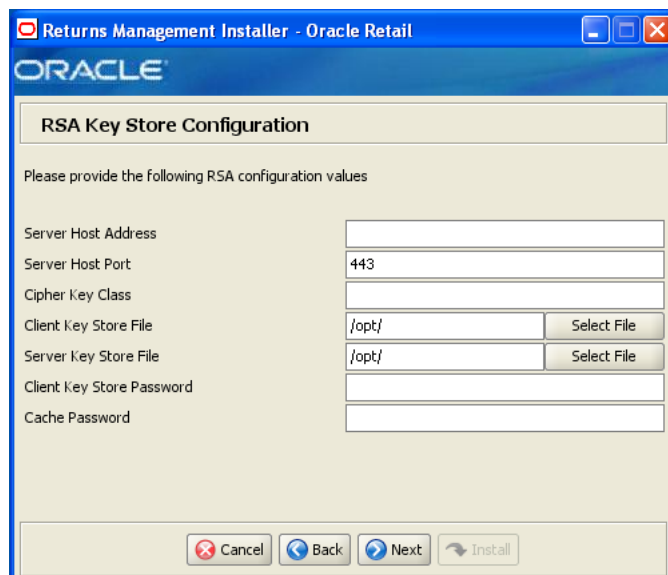


This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the RSA Key Manager interface.
Example	oracle.retail.stores.rsakeystore.rsainterface.RSAKeyStoreEncryptionService
Notes	

**Figure A–14 RSA Key Store Configuration**



This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Server Host Address
Field Description	Enter the IP address of the RSA server host.
Notes	

Field Title	Server Host Port
Field Description	Enter the port number for the RSA server host.
Example	443 443 is the default used by the RSA Key Manager.
Notes	

Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.
Notes	

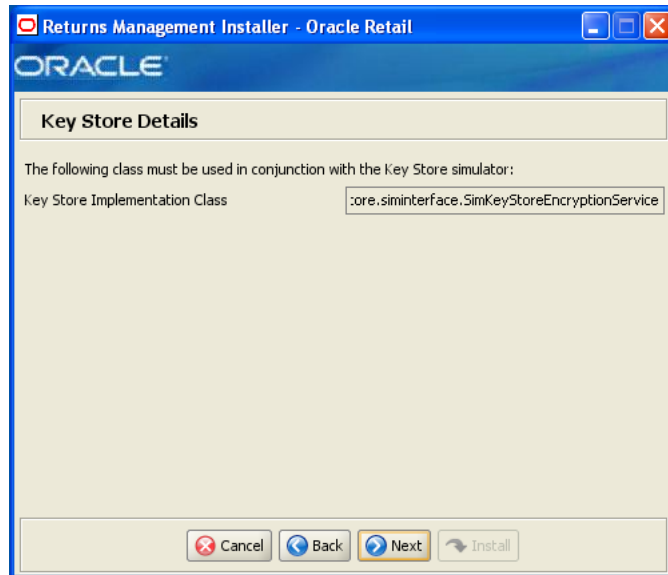
Field Title	Client Key Store File
Field Description	Select the location of the RSA Key Manager client Key Store file.
Notes	

Field Title	Server Key Store File
Field Description	Select the location of the RSA Key Manager server Key Store file.
Notes	

Field Title	Client Key Store Password
Field Description	Enter the password used to access the RSA Key Manager client Key Store.
Notes	

Field Title	Cache Password
Field Description	Enter the password used to access the RSA Key Manager cache.
Notes	

**Figure A–15 Key Store Details for Simulator Key Manager**

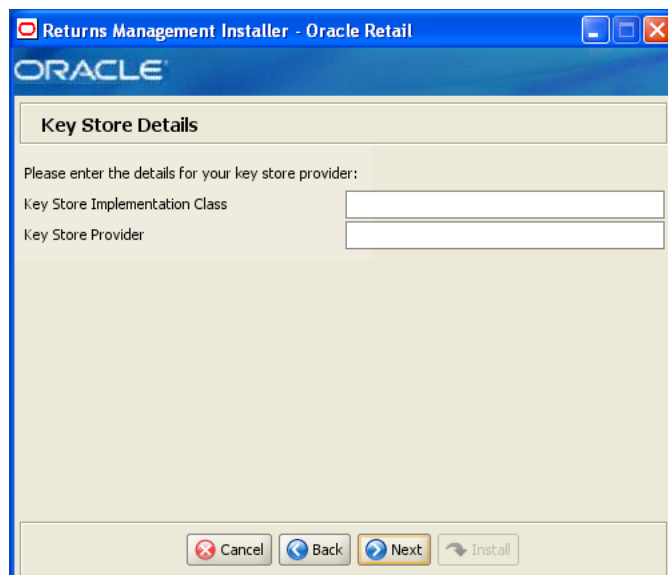


This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the simulated key manager interface.
Example	oracle.retail.stores.simkeystore.siminterface.SimKeyStoreEncryptionService
Notes	

**Figure A–16 Key Store Details for Other Key Manager**



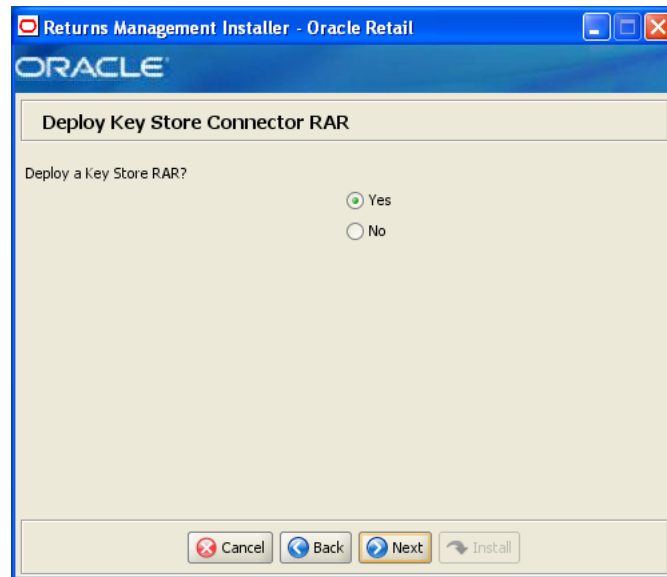
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the key manager interface.
Notes	

Field Title	Key Store Provider
Field Description	Enter the name of the provider for the Key Store.
Notes	

**Figure A-17 Deploy Key Store Connector RAR**



The field on this screen is described in the following table.

Field Title	Deploy a Key Store RAR?
Field Description	Select whether a Key Store RAR is to be deployed.
Example	Yes
Notes	

**Figure A–18 Key Store Connector RAR Details**

Returns Management Installer - Oracle Retail

ORACLE

**Key Store Connector RAR Details**

Enter the following information to deploy the Key Store Connector RAR:

Key Store Deployment Name: keystoreconnector

Key Store Connector RAR File: sa-keystoreconnector-rar.rar

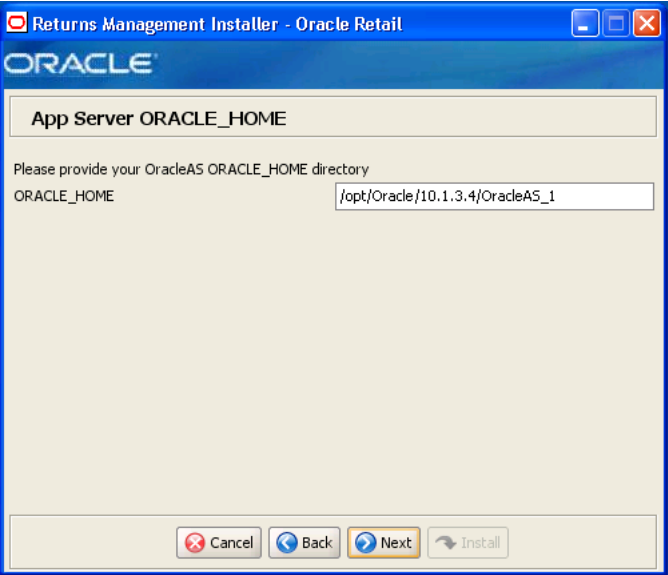
This screen is only displayed if **Yes** is selected on the Deploy Key Store Connector RAR screen. The fields on this screen are described in the following tables.

Field Title	Key Store Deployment Name
Field Description	Name to which the Key Store connector will be deployed.
Example	keystoreconnector
Notes	

Field Title	Key Store Connector RAR File
Field Description	Path name to the Key Store connector RAR file.
Example	/opt/connectors/keystoreconnector-rar.rar
Notes	



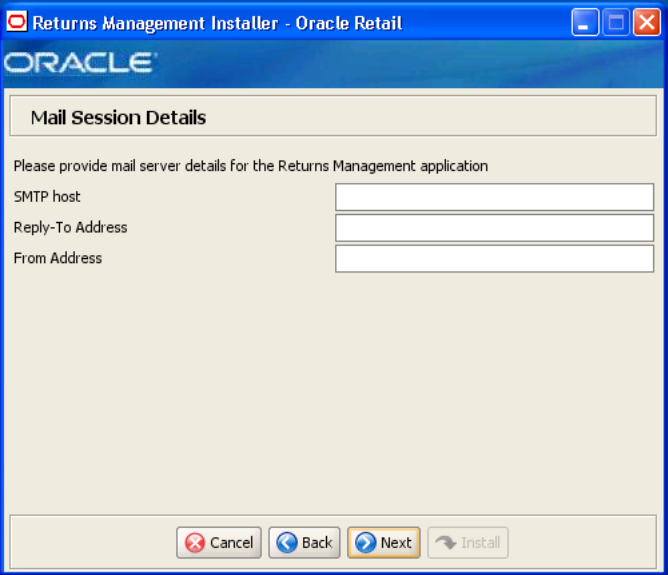
Figure A-19 App Server ORACLE\_HOME



The field on this screen is described in the following table.

Field Title	ORACLE_HOME
Field Description	ORACLE_HOME directory for the Oracle Application Server installation.
Example	/opt/oracle/product/10.1.3.4/OracleAS_1
Notes	

Figure A-20 Mail Session Details



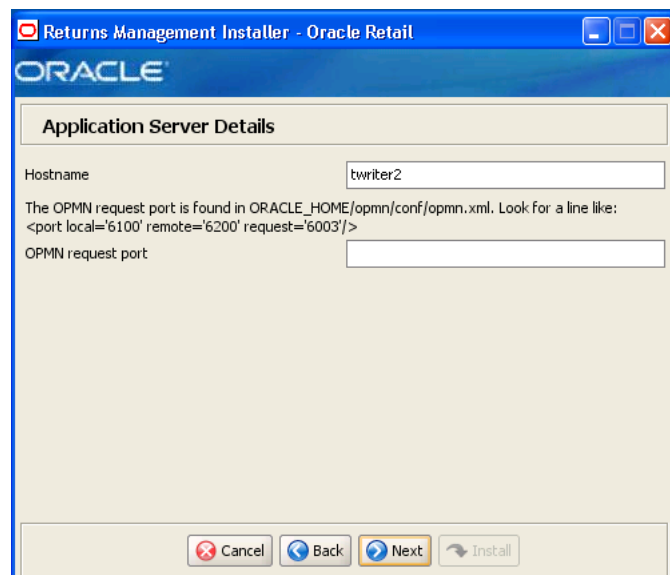
The fields on this screen are described in the following tables.

Field Title	SMTP host
Field Description	Host where the SMTP server is running.
Example	mail.mycompany.com
Notes	

Field Title	Reply-To Address
Field Description	Reply-to address in e-mails generated by Returns Management.
Example	donotreply@mycompany.com
Notes	

Field Title	From Address
Field Description	From address in e-mails generated by Returns Management.
Example	donotreply@mycompany.com
Notes	

**Figure A–21 Application Server Details**

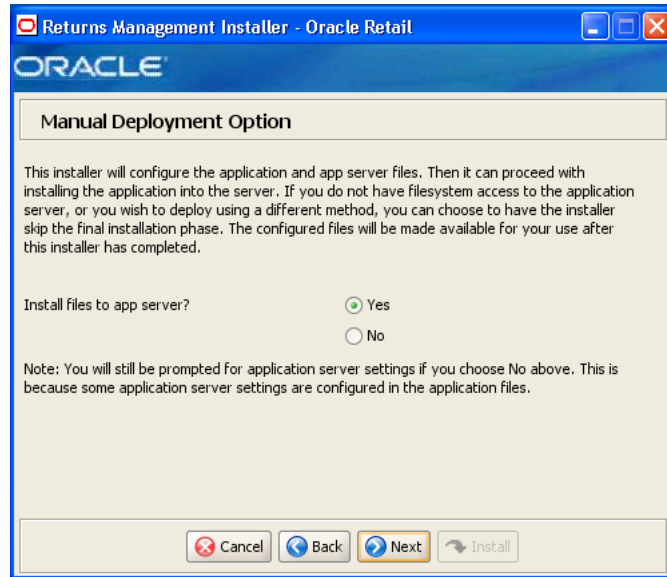


The fields on this screen are described in the following tables.

Field Title	Hostname
Field Description	Host name of the application server.
Example	twriter2
Notes	

Field Title	OPMN request port
Field Description	Port on which OPMN listens for requests to forward on to OC4J instances. This port can be found in the ORACLE_HOME/opmn/conf/opmn.xml file: <pre>&lt;port local="6100" remote="6200" request="6003"/&gt;</pre>
Example	6003
Notes	

**Figure A-22 Manual Deployment Option**



The field on this screen is described in the following table.

Field Title	Install files to app server?
Field Description	By default, the installer will deploy the ear file and copy files under the application server ORACLE_HOME. This screen gives you the option to leave ORACLE_HOME unmodified and configure the application in the staging area for use in a manual installation at a later time. This option can be used in situations where modifications to files under ORACLE_HOME must be reviewed by another party before being applied.  If you choose No, see <a href="#">"Manual Deployment of the Returns Management Application"</a> in <a href="#">Chapter 2</a> for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

**Figure A–23 Application Deployment Details**

**Returns Management Installer - Oracle Retail**

**Application Deployment Details**

The default values shown below are examples

Enter the deployment name for the Returns Management application. This is the name by which the application will be identified in the application server.

App Deployment Name: ReturnsManagement

Enter the web context root for this application. The web URL used to access the application will be http://server:port/contextroot/index.jsp

Context Root: returnsmanagement

Enter the name of the OC4J instance to which the Returns Management application will be deployed

OC4J instance: orrm-inst

Buttons: Cancel, Back, Next, Install

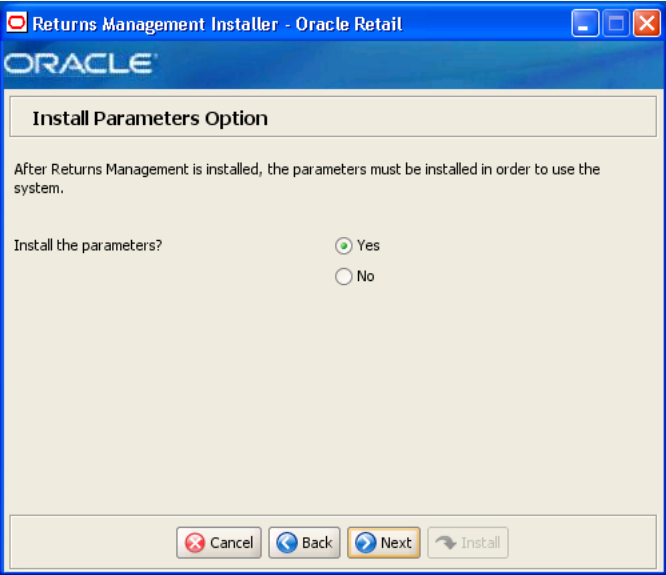
The fields on this screen are described in the following tables.

Field Title	App Deployment Name
Field Description	Name by which this Returns Management application will be identified in the application server.
Example	ReturnsManagement
Notes	

Field Title	Context Root
Field Description	Path under the HTTP URL that will be used to access the Returns Management application. For example, a context root of 'returnsmanagement' will result in the application being accessed at https://<host>:<port>/returnsmanagement/index.jsp.
Example	returnsmanagement
Notes	

Field Title	OC4J Instance
Field Description	Name of the OC4J instance that was created for this Returns Management application.
Example	orrm-inst
Notes	

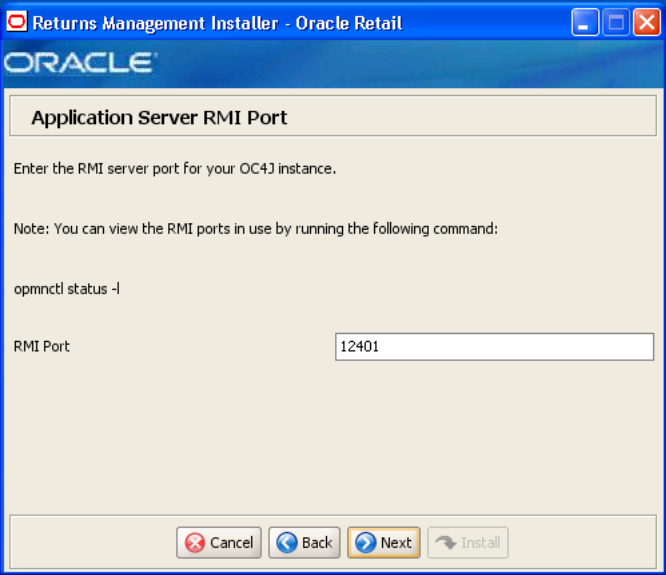
Figure A-24 Install Parameters Option



The field on this screen is described in the following table.

Field Title	Install the parameters?
Field Description	The application parameters must be set up before Returns Management can be used. This screen gives you the option to set up the parameters manually. If you choose No, see <a href="#">"Install Parameters Option"</a> in <a href="#">Chapter 2</a> for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

Figure A-25 Application Server RMI Port



This screen is only displayed if **Yes** is selected for the Install the Parameters option. The field on this screen is described in the following table.

Field Title	RMI Port
Field Description	Port to be used for installing parameters. This port can be found in the ORACLE_HOME/opmn/conf/opmn.xml file.
Example	12401
Notes	

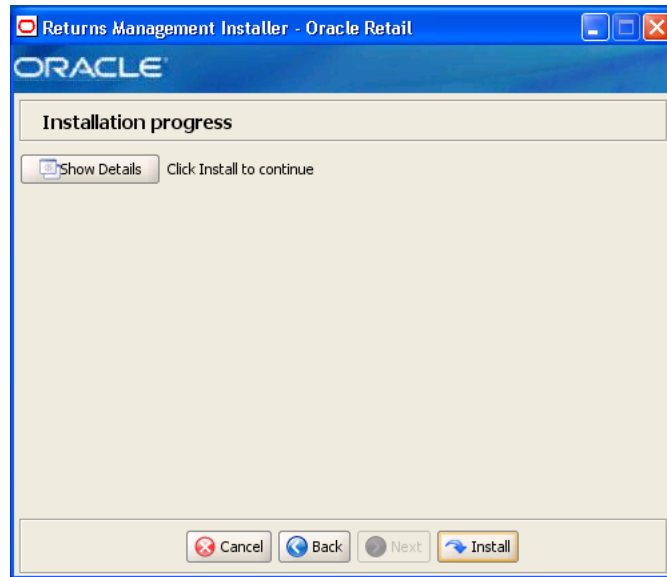
**Figure A-26 OC4J Administrative User**

The fields on this screen are described in the following tables.

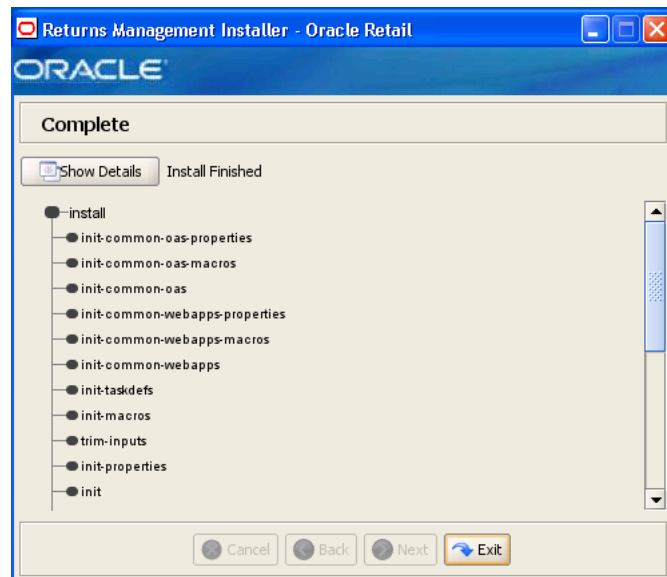
Field Title	OC4J admin user
Field Description	Username of the admin user for OC4J instance to which the Returns Management application is being deployed.
Example	oc4jadmin
Notes	

Field Title	OC4J admin password
Field Description	Password for the OC4J admin user. You chose this password when you created the OC4J instance.
Notes	

**Figure A–27 Installation Progress**



**Figure A–28 Installation Complete**



After the installer completes, the Oracle Configuration Manager (OCM) installer runs if OCM is not already installed. For information on OCM, see ["Oracle Configuration Manager"](#) in [Chapter 2](#).





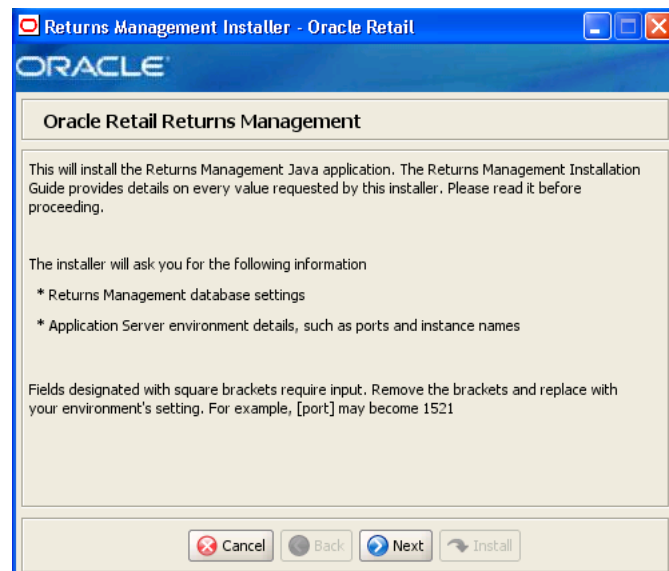
---

## Appendix: Returns Management Application Installer Screens for the IBM Stack on IRES

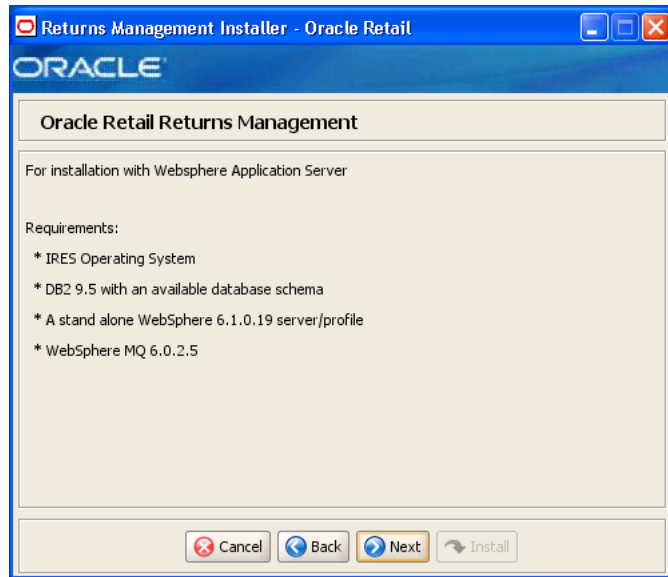
You need the following details about your environment for the installer to successfully deploy the Returns Management application on the IBM stack on IRES. Depending on the options you select, you may not see some screens or fields.

For each field on a screen, a table is included in this appendix that describes the field. If you want to document any specific information about your environment for any field, a Notes row is provided in each table for saving that information.

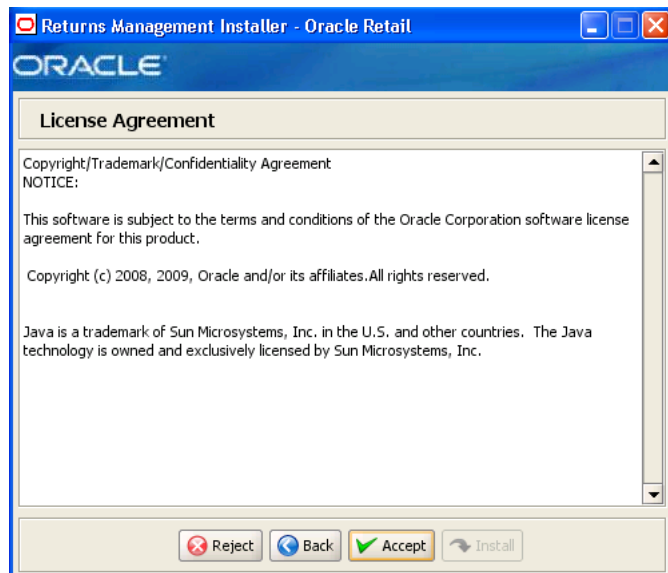
**Figure B-1** Introduction



**Figure B–2 Requirements**



**Figure B–3 License Agreement**

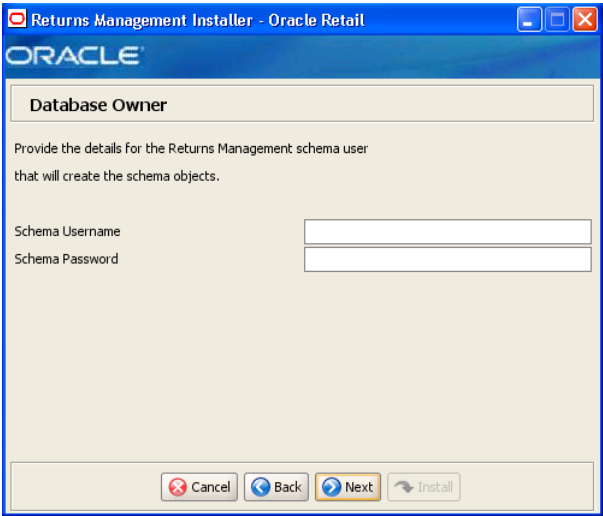


---

**Note:** You must choose to accept the terms of the license agreement in order for the installation to continue.

---

Figure B-4 Database Owner



The fields on this screen are described in the following tables.

Field Title	Schema Username
Field Description	Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see <a href="#">"Create the Database Schema Owner and Data Source Users"</a> in <a href="#">Chapter 3</a> .  <b>Note:</b> This user creates the database objects used by Returns Management.
Example	DBOWNER
Notes	

Field Title	Schema Password
Field Description	Password for the database owner.
Notes	

**Figure B–5 Data Source User**

Oracle Retail Returns Management Installer - Oracle Retail

**Data Source User**

Provide the details for the Returns Management schema user

JDBC URL: jdbc:db2://[host]:[tcpPort]/[dbname]

Data Source Username: [ ]

Data Source Password: [ ]

Buttons: Cancel, Back, Next, Install

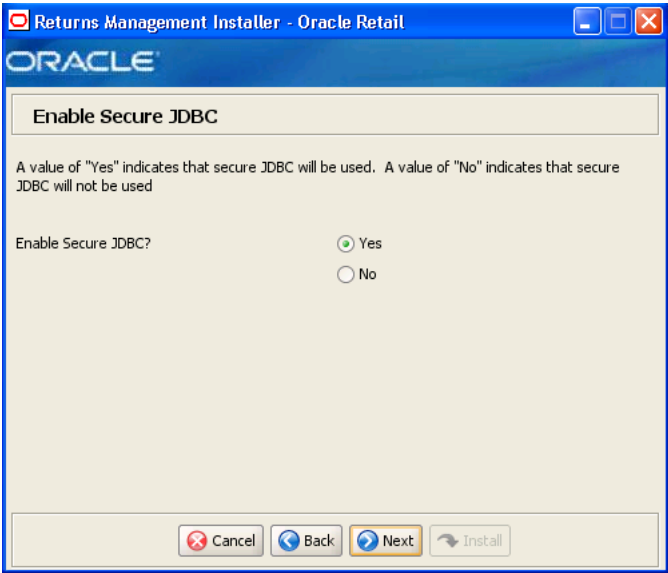
The fields on this screen are described in the following tables.

Field Title	JDBC URL
Field Description	URL used by the Returns Management application to access the database schema. See <a href="#">Appendix E</a> for the expected syntax.
Example	jdbc:db2://myhost:50000/mydb
Notes	

Field Title	Data Source Username
Field Description	Database user name that can access and manipulate the data in the schema. This user can have Select, Insert, Update, Delete, and Execute privileges on objects in the schema, that is, Data Manipulation Language (DML) execution privileges. For information on creating this user, see <a href="#">"Create the Database Schema Owner and Data Source Users"</a> in <a href="#">Chapter 3</a> .  <b>Note:</b> This schema user is used by Returns Management to access the database.
Example	DBUSER
Notes	

Field Title	Data Source Password
Field Description	Password for the data source user.
Notes	

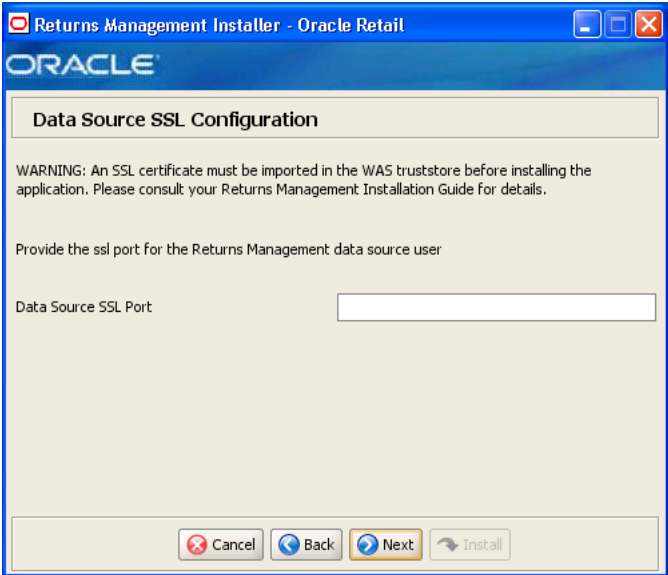
**Figure B–6 Enable Secure JDBC**



The field on this screen is described in the following table.

Field Title	Enable Secure JDBC?
Field Description	Select whether secure JDBC is to be used for communication with the database.
Example	Yes
Notes	

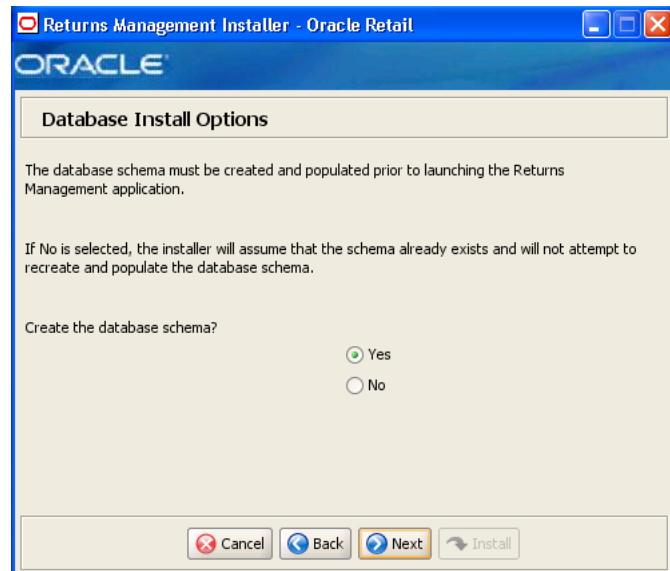
**Figure B–7 Data Source SSL Configuration**



This screen is only displayed if **Yes** is selected on the Enable Secure JDBC screen. The field on this screen is described in the following table.

Field Title	Data Source SSL Port
Field Description	SSL port used to access the database.
Example	1521
Notes	

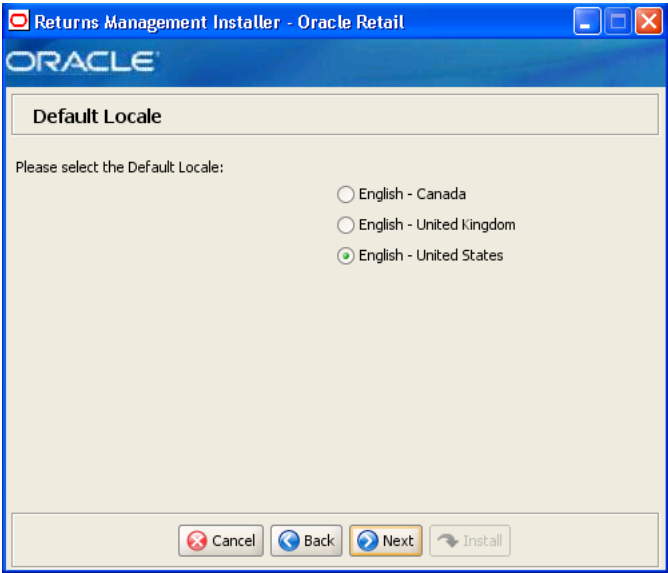
**Figure B–8 Database Install Options**



The field on this screen is described in the following table.

Field Title	Create the database schema?
Field Description	<p>The database schema must be created and populated before starting Returns Management. This screen gives you the option to have the installer create and populate the database schema or leave the database schema unmodified.</p> <ul style="list-style-type: none"> <li>■ To have the installer create and populate the database schema, select <b>Yes</b>.</li> <li>■ To have the installer leave the database schema unchanged, select <b>No</b>.</li> </ul> <p>For more information, see "<a href="#">Database Install Options</a>" in <a href="#">Chapter 3</a>.</p>
Example	Yes
Notes	

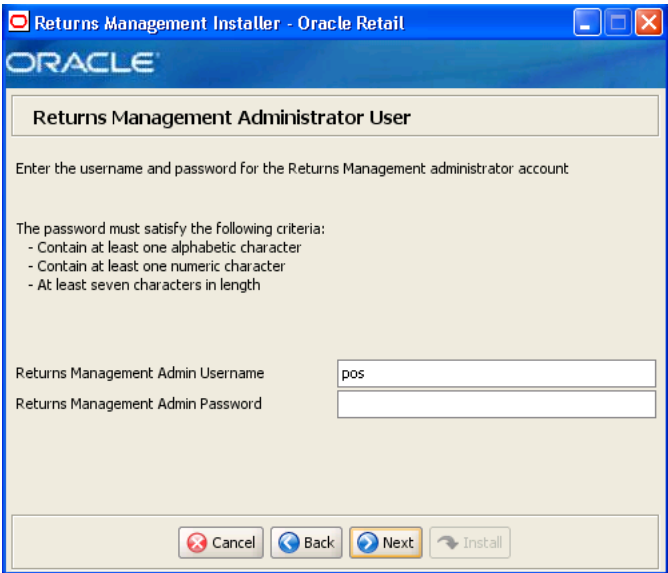
Figure B–9 Default Locale



The field on this screen is described in the following table.

Field Title	Please select the Default Locale
Field Description	Limited locale support in Returns Management enables the date, time, currency, and calendar to be displayed in the format for the selected default locale.  <b>Note:</b> The only language currently supported is United States English.
Example	English - United States
Notes	

Figure B–10 Returns Management Administrator User

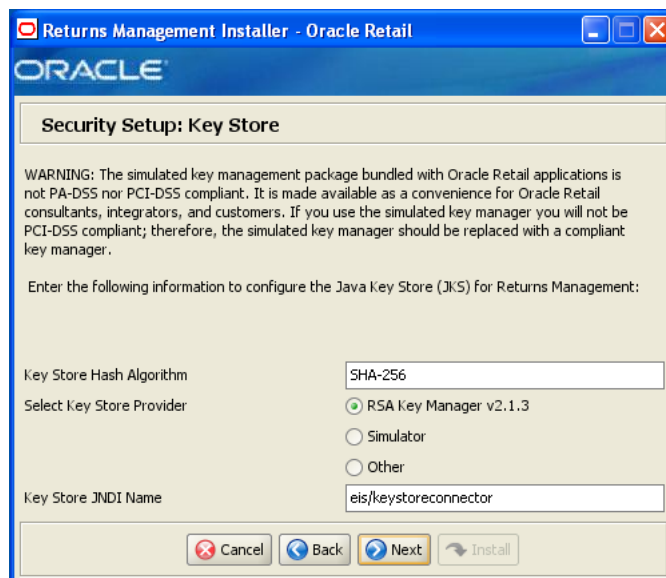


The fields on this screen are described in the following tables.

Field Title	Returns Management Administrator Username
Field Description	User name used for performing Returns Management administrative functions.
Example	pos
Notes	

Field Title	Returns Management Administrator Password
Field Description	Password for the administrator user.
Notes	

**Figure B–11 Security Setup: Key Store**



The fields on this screen are described in the following tables.

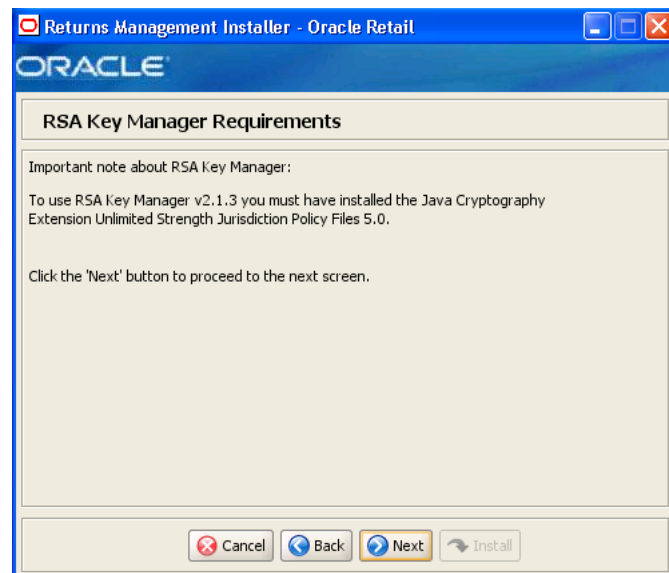
Field Title	KeyStore Hash Algorithm
Field Description	Name of the algorithm used by the Key Store to hash sensitive data.
Example	SHA-256
Notes	



Field Title	Select Key Store Provider
Field Description	<p>Provider for Key Store management.</p> <ul style="list-style-type: none"> <li>To use the RSA key management package, select <b>RSA Key Manager v2.1.3</b>. The next screen displayed is <a href="#">Figure B-12</a>.</li> <li>To use the simulated key management package, select <b>Simulator</b>. The next screen displayed is <a href="#">Figure B-15</a>.</li> <li>To use a different key management provider, select <b>Other</b>. The next screen displayed is <a href="#">Figure B-16</a>.</li> </ul>
Example	RSA Key Manager v2.1.3
Notes	

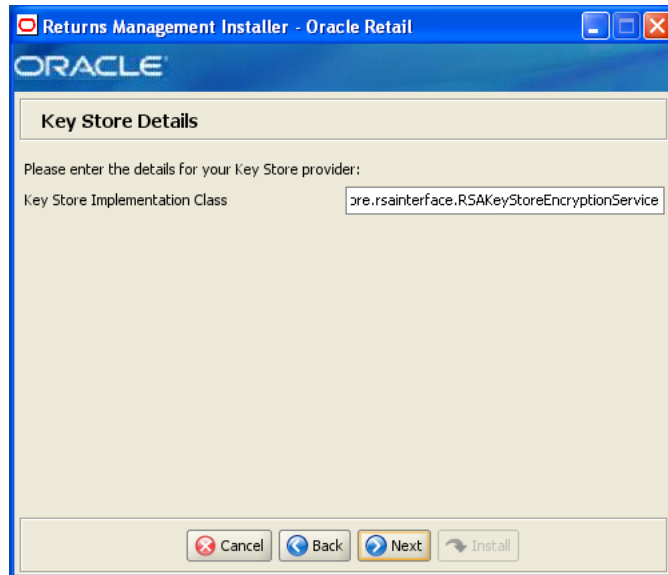
Field Title	Key Store JNDI Name
Field Description	Name of the Key Store JNDI.
Example	eis/keystoreconnector
Notes	

**Figure B-12 RSA Key Manager Requirements**



This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

**Figure B–13 Key Store Details for RSA Key Manager 2.1.3**

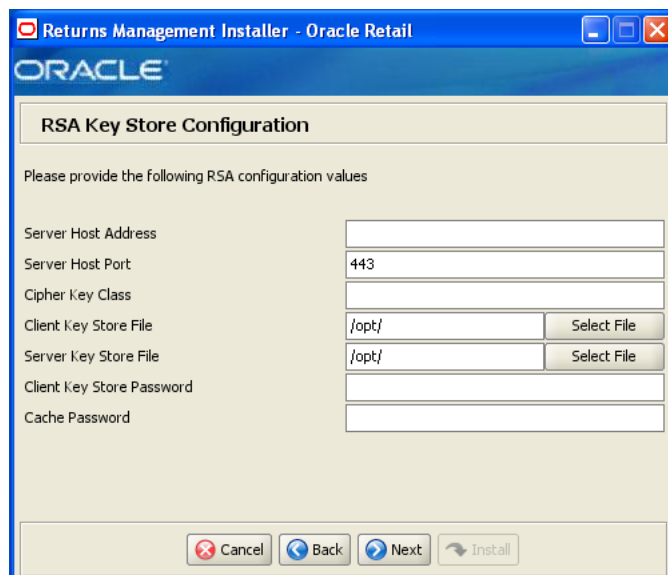


This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the RSA Key Manager interface.
Example	oracle.retail.stores.rsakeystore.rsainterface.RSAKeyStoreEncryptionService
Notes	

**Figure B–14 RSA Key Store Configuration**



This screen is only displayed if **RSA Key Manager v2.1.3** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Server Host Address
Field Description	Enter the IP address of the RSA server host.
Notes	

Field Title	Server Host Port
Field Description	Enter the port number for the RSA server host.
Example	443 443 is the default used by the RSA Key Manager.
Notes	

Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.
Notes	

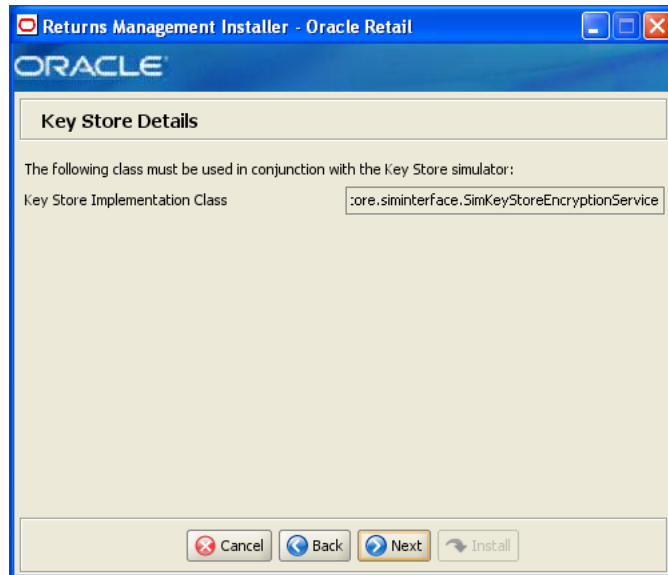
Field Title	Client Key Store File
Field Description	Select the location of the RSA Key Manager client Key Store file.
Notes	

Field Title	Server Key Store File
Field Description	Select the location of the RSA Key Manager server Key Store file.
Notes	

Field Title	Client Key Store Password
Field Description	Enter the password used to access the RSA Key Manager client Key Store.
Notes	

Field Title	Cache Password
Field Description	Enter the password used to access the RSA Key Manager cache.
Notes	

**Figure B–15 Key Store Details for Simulator Key Manager**

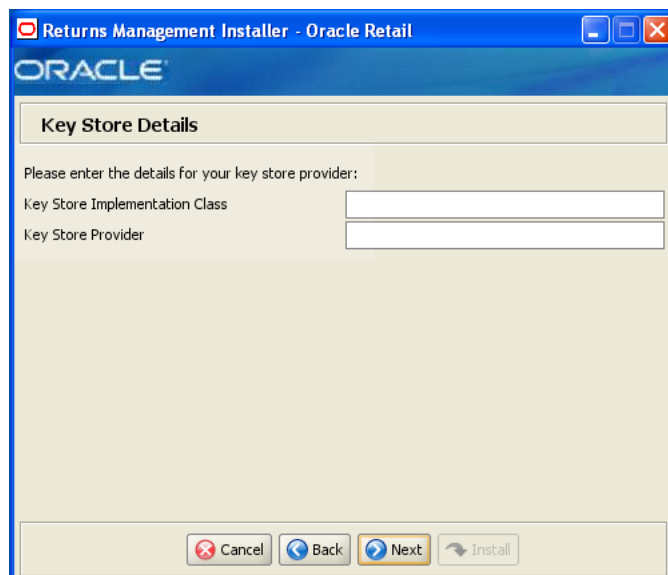


This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the simulated key manager interface.
Example	oracle.retail.stores.simkeystore.siminterface.SimKeyStoreEncryptionService
Notes	

**Figure B–16 Key Store Details for Other Key Manager**



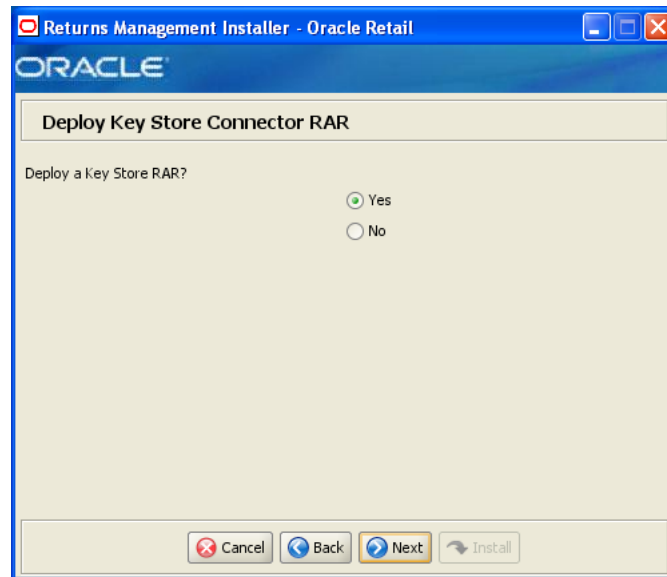
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the key manager interface.
Notes	

Field Title	Key Store Provider
Field Description	Enter the name of the provider for the Key Store.
Notes	

**Figure B–17** *Deploy Key Store Connector RAR*



The field on this screen is described in the following table.

Field Title	Deploy a Key Store RAR?
Field Description	Select whether a Key Store RAR is to be deployed.
Example	Yes
Notes	

**Figure B–18 Key Store Connector RAR Details**

Returns Management Installer - Oracle Retail

ORACLE

**Key Store Connector RAR Details**

Enter the following information to deploy the Key Store Connector RAR:

Key Store Deployment Name: keystoreconnector

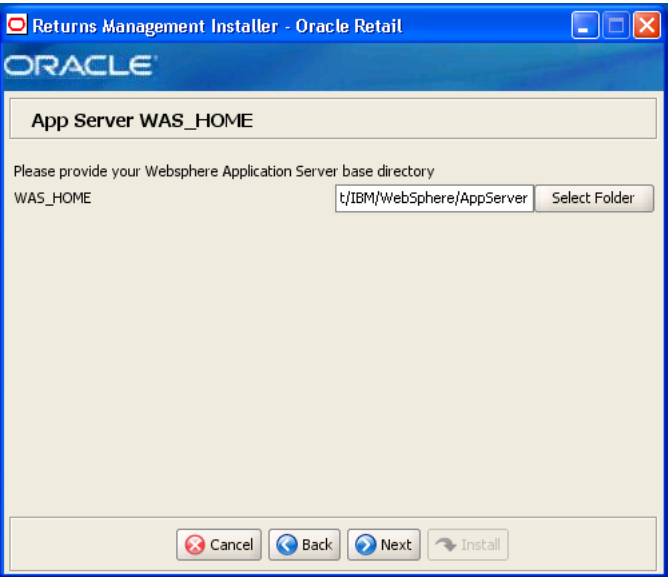
Key Store Connector RAR File: sa-keystoreconnector-rar.rar

This screen is only displayed if **Yes** is selected on the Deploy Key Store Connector RAR screen. The fields on this screen are described in the following tables.

Field Title	Key Store Deployment Name
Field Description	Name to which the Key Store connector will be deployed.
Example	keystoreconnector
Notes	

Field Title	Key Store Connector RAR File
Field Description	Path name to the Key Store connector RAR file.
Example	/opt/connectors/keystoreconnector-rar.rar
Notes	

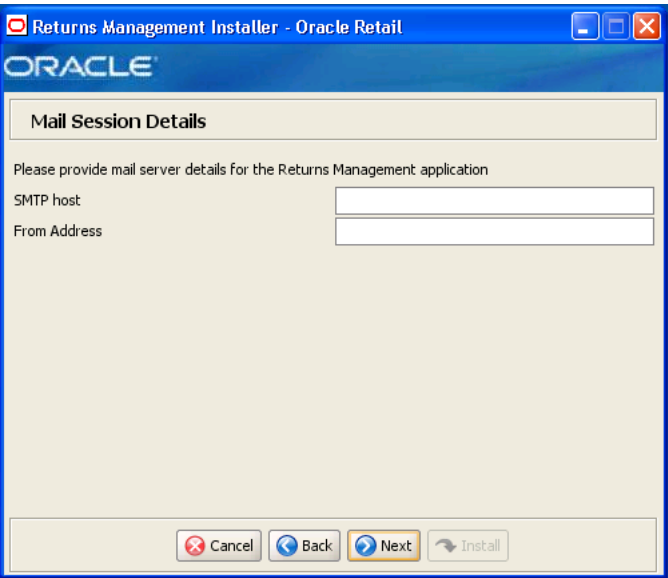
Figure B-19 App Server WAS\_HOME



The field on this screen is described in the following table.

Field Title	WAS_HOME
Field Description	Base directory for the IBM WebSphere Application Server installation.
Example	/opt/IBM/WebSphere/AppServer
Notes	

Figure B-20 Mail Session Details



The fields on this screen are described in the following tables.

Field Title	SMTP host
Field Description	Host where the SMTP server is running.
Example	mail.mycompany.com
Notes	

Field Title	From Address
Field Description	From address in e-mails generated by Returns Management.
Example	donotreply@mycompany.com
Notes	

**Figure B–21 Application Server Details**

The screenshot shows a window titled "Returns Management Installer - Oracle Retail". Inside, there's a tab labeled "Application Server Details". The form has the following fields:

- Server Name: server1
- Node Name: (empty)
- Cell Name: (empty)
- IIOP Port: 2809
- Server Profile: (empty)
- Timezone: America/Chicago

At the bottom, there are four buttons: "Cancel", "Back", "Next", and "Install".

The fields on this screen are described in the following tables.

Field Title	Server Name
Field Description	Name of the IBM WebSphere server.
Example	server1
Notes	

Field Title	Node Name
Field Description	Name of the IBM WebSphere node.
Example	myhostNode01
Notes	



Field Title	Cell Name
Field Description	Name of the IBM WebSphere cell.
Example	myhostNode01Cell
Notes	

Field Title	IIOP port
Field Description	IIOP/BOOTSTRAP_ADDRESS port of the IBM WebSphere server. This port can be found in the <code>&lt;WAS_HOME&gt;/profiles/&lt;profile name&gt;/properties/portdef.props</code> file.
Example	2809
Notes	

Field Title	Server Username
Field Description	User name for the IBM WebSphere server. This user must exist in the Returns Management schema.
Example	myuser
Notes	

Field Title	Server Password
Field Description	Password for the IBM WebSphere server.
Notes	

Field Title	Server Profile
Field Description	Name of the IBM WebSphere profile.
Example	AppSrv01
Notes	

Field Title	Timezone
Field Description	Time zone where this server is running.
Example	America/Chicago
Notes	

**Figure B-22 JMS Server Details**

The screenshot shows a window titled "Returns Management Installer - Oracle Retail". Inside, there's a section titled "JMS Server Details". It contains five text input fields: "JMS Host Name", "JMS Port", "JMS Username", "JMS Password", and "JMS Queue Manager". The "JMS Queue Manager" field is populated with the text "rm.queue.manager". At the bottom of the window, there are four buttons: "Cancel", "Back", "Next", and "Install". The "Next" button is highlighted with a yellow border.

The fields on this screen are described in the following tables.

Field Title	JMS Server Name
Field Description	Name of the JMS server. <b>Note:</b> Always use the actual hostname and not the IP address or "localhost". There may be problems integrating with Oracle Retail Point-of-Service if the actual hostname is not used.
Example	myhost
Notes	

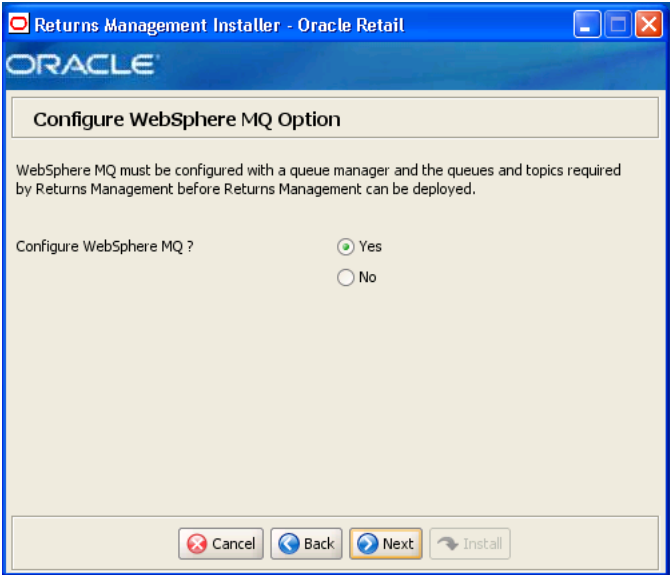
Field Title	JMS Server Port
Field Description	Port number used by the JMS server.
Example	1414
Notes	

Field Title	JMS Username
Field Description	User name for the JMS server. This user must exist in the operating system. It must be the same user that is used for IBM WebSphere MQ.
Example	mqm
Notes	

Field Title	JMS Password
Field Description	Password for the JMS server.
Notes	

Field Title	JMS Queue Manager
Field Description	Name of the JMS queue manager.
Example	rm.queue.manager
Notes	

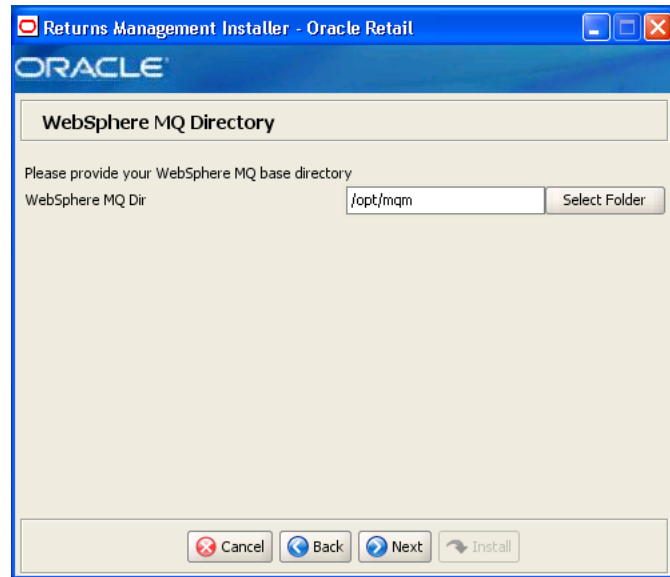
**Figure B-23** *Configure MQ Server Option*



The field on this screen is described in the following table.

Field Title	Configure MQ Server?
Field Description	MQ Server must be configured with a queue manager and the queues and topics required by Returns Management before Returns Management can be deployed. This screen gives you the option to configure MQ Server manually. If you choose No, see <a href="#">"Configure IBM WebSphere MQ"</a> in <a href="#">Chapter 3</a> for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

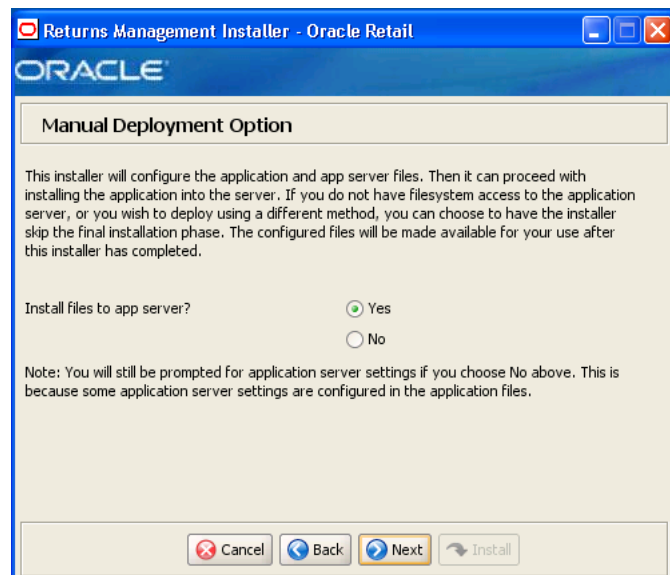
**Figure B–24 MQ Server Directory**



This screen is only displayed if **Yes** is selected on the Configure MQ Server Option screen. The field on this screen is described in the following table.

Field Title	MQ Dir
Field Description	Base directory for MQ Server.
Example	/opt/mqm
Notes	

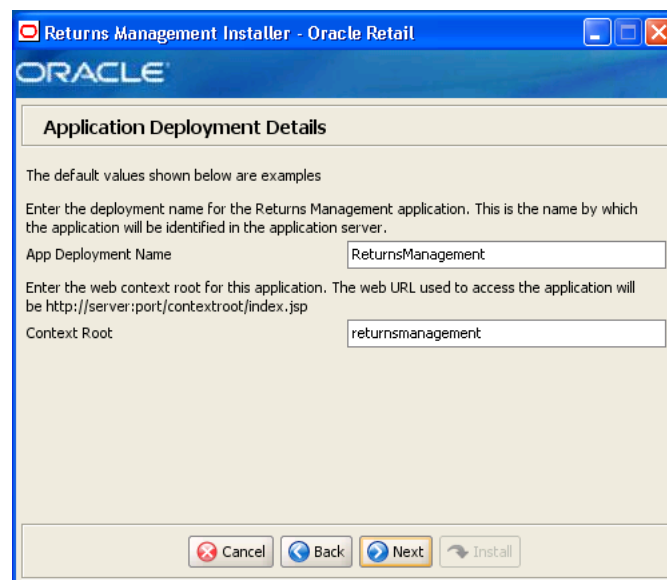
**Figure B–25 Manual Deployment Option**



The field on this screen is described in the following table.

Field Title	Install files to app server?
Field Description	By default, the installer will deploy the ear file. This screen gives you the option to configure the application in the staging area for use in a manual installation at a later time. This option can be used in situations where modifications to the deployed files must be reviewed by another party before being applied.  If you choose No, see <a href="#">"Manual Deployment of the Returns Management Application"</a> in <a href="#">Chapter 3</a> for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

**Figure B–26 Application Deployment Details**

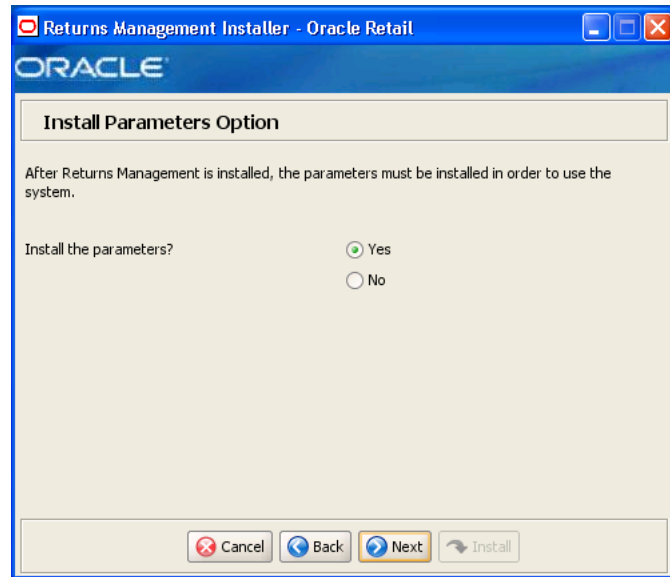


The fields on this screen are described in the following tables.

Field Title	App Deployment Name
Field Description	Name by which this Returns Management application will be identified in the application server.
Example	ReturnsManagement
Notes	

Field Title	Context Root
Field Description	Path under the HTTP URL that will be used to access the Returns Management application. For example, a context root of 'returnsmanagement' will result in the application being accessed at <code>http://&lt;host name&gt;:&lt;port number&gt;/returnsmanagement/</code> .
Example	returnsmanagement
Notes	

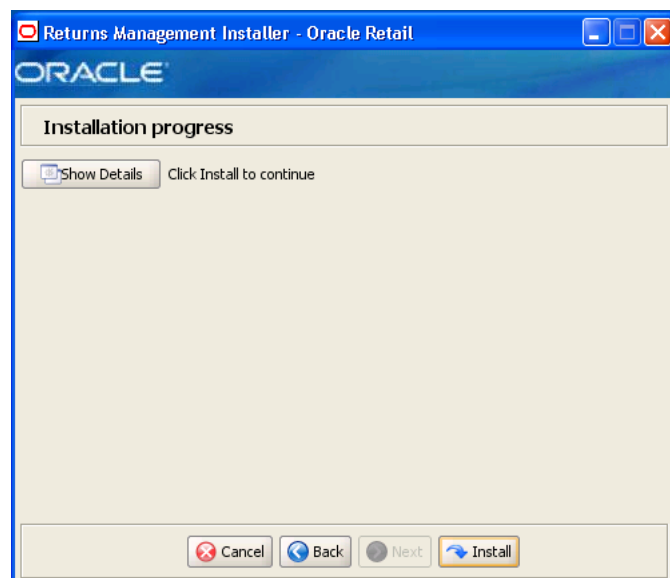
**Figure B–27 Install Parameters Option**



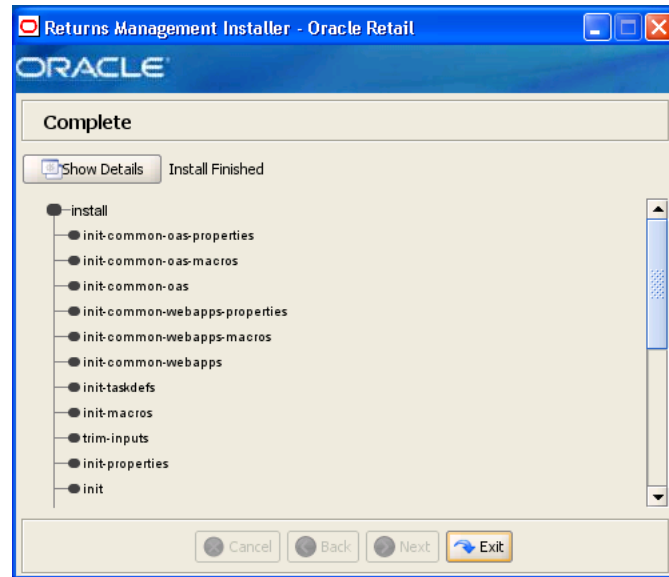
The field on this screen is described in the following table.

Field Title	Install the parameters?
Field Description	The application parameters must be set up before Returns Management can be used. This screen gives you the option to set up the parameters manually. If you choose No, see <a href="#">"Install Parameters" in Chapter 3</a> for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

**Figure B–28 Installation Progress**



**Figure B–29 Installation Complete**



After the installer completes, the Oracle Configuration Manager (OCM) installer runs if OCM is not already installed. For information on OCM, see ["Oracle Configuration Manager"](#) in [Chapter 3](#).





---

## Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the Returns Management installer, there is a silent mode that can be run. This mode is useful if you wish to run a repeat installation without reentering the settings you provided in the previous installation. It is also useful if you encounter errors in the middle of an installation and wish to continue after resolving them.

The installer runs in two distinct phases. The first phase involves gathering settings from the user. At the end of the first phase, a properties file named `ant.install.properties` is created with the settings that were provided. In the second phase, this properties file is used to provide your settings for the installation.

To skip the first phase and re-use the `ant.install.properties` file from a previous run, follow these instructions:

1. Edit the `ant.install.properties` file and correct any invalid settings that may have caused the installer to fail in its previous run.
2. Run the installer again with the silent argument.

```
install.sh [silent oracle | websphere]
```



---

## Appendix: Reinstalling Returns Management

Returns Management does not provide the capability to uninstall and reinstall the application. If you need to run the Returns Management installer again, perform the following steps.

### Reinstalling Returns Management on the Oracle Stack

To reinstall:

1. Stop the OC4J Returns Management instance.
2. Delete the instance.
3. Recreate the OC4J Returns Management instance.
4. Start the instance.
5. Run the Returns Management installer. For more information, see "[Run the Returns Management Application Installer](#)" in [Chapter 2](#).

### Reinstalling Returns Management on the IBM Stack

To reinstall:

1. Stop the WebSphere application server in the profile that contains Returns Management.
2. Delete the profile.
3. Stop the WebSphere MQ queue manager (for example, `rm.queue.manager`) and listener.
4. Delete the queue manager.
5. Recreate the profile.
6. Start the WebSphere application server in the profile.
7. Run the Returns Management installer. For more information, see "[Run the Returns Management Application Installer](#)" in [Chapter 3](#).



---

## Appendix: URL Reference

Both the database schema and application installers for the Returns Management product will ask for several different URLs. These include the following.

### URLs for the Oracle Stack

The following URLs are used for the Oracle stack.

### JDBC URL for a Database

Used by the Java application and by the installer to connect to the database.

Syntax: `jdbc:oracle:thin:@<host>:<port>:<sid>`

- `<host>`: hostname of the database server
- `<port>`: database listener port
- `<sid>`: system identifier for the database

For example, `jdbc:oracle:thin:@myhost:1525:mysid`

### JNDI Provider URL for an Application

Used for server-to-server calls between applications.

Syntax: `opmn:ormi://<host>:<port>:<instance>/<app>`

- `<host>`: hostname of the OracleAS environment
- `<port>`: OPMN request port of the OracleAS environment. This can be found in the `<ORACLE_HOME>/opmn/conf/opmn.xml` file
- `<instance>`: name of the OC4J instance running the application
- `<app>`: deployment name for the application

For example,

`opmn:ormi://localhost:12401:orrm-inst/ReturnsManagement`

---

**Note:** The JNDI provider URL can have a different format depending on your cluster topology. Consult the Oracle Application Server documentation for further details.

---

## Deployer URI

Used by the Oracle Ant tasks to deploy an application to an OC4J instance. The application installer does not ask the user for this value. It is constructed based on other inputs and written to the `ant.install.properties` file for input to the installation script. For repeat installations using silent mode, you may need to correct mistakes in the deployer URI.

---

**Note:** There are several different formats for the deployer URI depending on your cluster topology. Consult the Deploying with the OC4J Ant Tasks chapter of the *OC4J Deployment Guide* for further details.

---

Syntax (managed OC4J):

`deployer:cluster:opmn://<host>:<port>/<instance>`

- `<host>`: hostname of the OracleAS environment
- `<port>`: OPMN request port of the OracleAS environment. This can be found in the `<ORACLE_HOME>/opmn/conf/opmn.xml` file.
- `<instance>`: name of the OC4J instance where the application will be deployed

For example, `deployer:OC4J:opmn://localhost:6004/home`

## URLs for the IBM Stack

The following URLs are used for the IBM stack.

### JDBC URL for a Database

Used by the Java application and by the installer to connect to the database.

Syntax: `jdbc:db2://<dbhost>:<dbport>/<dbname>`

- `<dbhost>`: hostname of the database server
- `<dbport>`: database listener port
- `<dbname>`: system identifier for the database

For example, `jdbc:db2://myhost:50000/mydatabase`

### JNDI Provider URL for an Application

Used for server-to-server calls between applications.

Syntax: `corbaloc:iiop:<host>:<iiopport>`

- `<host>`: hostname of the WebSphere server
- `<iiopport>`: IIOP/BOOTSTRAP\_ADDRESS port of the WebSphere server. This can be found in the `<WAS_HOME>/profiles/<profile_name>/properties/portdef.props` file.

For example, `corbaloc:iiop:myhost:2809`

---

## Appendix: Common Installation Errors

---

This appendix describes some common errors encountered during installation of Returns Management.

### Unreadable Buttons in the Installer

If you are unable to read the text within the installer buttons, it probably means that your `JAVA_HOME` points to a pre-1.5 JDK. Set `JAVA_HOME` to a Java development kit of version 1.5 or later and run the installer again.

### Installation Errors for the Oracle Stack

The following errors only occur when installing for the Oracle Stack.

#### Oracle Application Server Forceful Shutdown

If an error occurs during installation, Oracle Application Server may not shutdown gracefully but will instead do a forceful shutdown. This is a known problem with Oracle Application Server.

You can use `opmnctl status` to check if the application server has stopped appropriately.

#### OC4J Instance Does Not Exist

##### Symptom:

The application installer quits with the following error message:

```
BUILD FAILED
```

```
C:\tmp\j2ee\rm\staging\ORRM-trunk\build.xml:697: The following error occurred
while executing this line:
C:\tmp\j2ee\rm\staging\ORRM-trunk\build-common-oas.xml:107: Exiting. OC4J instance
orrm-inst does not exist
```

##### Solution:

This error occurs because the OC4J instance provided does not exist.

Make sure that the OC4J instance exists, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the `input.deployer.uri` (see [Appendix F](#)), `input.oc4j.instance`, `input.admin.user`, and `input.admin.password` properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see [Appendix D](#)).

## OC4J Instance is Not Started

### Symptom:

The application installer quits with the following error message:

```
BUILD FAILED
```

```
C:\tmp\j2ee\rm\staging\ORRM-trunk\build.xml:730: The following error occurred
while executing this line:
C:\tmp\j2ee\rm\staging\ORRM-trunk\build-common-oas.xml:115: Exiting. OC4J instance
orrm-inst exists but is not alive
```

### Solution:

This error occurs because the OC4J instance provided is not running.

Make sure that the OC4J instance is running, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the `input.deployer.uri` (see [Appendix F](#)), `input.oc4j.instance`, `input.admin.user`, and `input.admin.password` properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see [Appendix D](#)).

## "Unable to get a deployment manager" Message

### Symptom:

The application installer quits with the following error message:

```
[oracle:deploy] Unable to get a deployment manager.
[oracle:deploy]
[oracle:deploy] This is typically the result of an invalid deployer URI format
being supplied, the target server not being in a started state or incorrect
authentication details being supplied.
[oracle:deploy]
[oracle:deploy] More information is available by enabling logging -- please see
the Oracle Containers for J2EE Configuration and Administration Guide for details.
```

### Solution:

This error can be caused by any of the following conditions:

- OC4J instance provided is not running
- Incorrect OC4J instance name provided
- Incorrect OC4J administrative username, password, or both
- Incorrect OPMN request port provided

Make sure that the OC4J instance is running, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the `input.deployer.uri` (see [Appendix E](#)), `input.oc4j.instance`, `input.admin.user`, and `input.admin.password` properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see [Appendix C](#)).



## "Could not create system preferences directory" Warning

### Symptom:

The following text appears in the installer Errors tab:

```
[May 22, 2006 11:16:39 AM java.util.prefs.FileSystemPreferences$3 run
WARNING: Could not create system preferences directory. System preferences are
unusable.
May 22, 2006 11:17:09 AM java.util.prefs.FileSystemPreferences
checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code -264946424]
```

### Solution:

This is related to Java bug 4838770. The `/etc/.java/.systemPrefs` directory may not have been created on your system. See <http://bugs.sun.com> for details.

This is an issue with your installation of Java and does not affect the Oracle Retail product installation.

## Installation Hangs at "Compiling EJB generated code"

### Symptom:

The installer freezes for 10 minutes or more showing this as the last message:

```
[[myinstance.name] 06/11/17 16:51:57 Notification ==>Compiling EJB generated code]
```

### Solution:

Before cancelling the installation, check the OC4J log file. This file is usually located under `$ORACLE_HOME/opmn/logs` and is named after the OC4J instance. This could be a memory problem if you did not follow the steps to set the PermSize space. See ["Create a New OC4J Instance for Returns Management"](#) in [Chapter 2](#).

## "Failed to set the internal configuration" Message

### Symptom:

The following text appears in the log file:

```
07/03/19 14:34:51 *** (SEVERE) Failed to set the internal configuration of the
OC4J JMS Server with: XMLJMServerConfig[file:/u01/10.1.3/OracleAS_1/
j2ee/home/config/jms.xml]
```

### Solution:

Check the OC4J log file. This file is usually located under `$ORACLE_HOME/opmn/logs` and is named after the OC4J instance. A `NameNotFoundException` for `jms/XAQueueConnectionFactory` appears in the log.

To resolve the problem, do the following:

1. Shutdown the application server.
2. Delete the `OracleAS_1/j2ee/<OC4J instance>/persistence/<OC4J instance>_default_group_1/*.lock` file.
3. Restart the application server.



---

## Appendix: Returns Data Loader

The Oracle Retail Returns Management installation includes return ticket data, in XML format, which you can optionally load into the Returns Management database. There are several reasons why you would want to load this data:

- Once return tickets are loaded into the database, you can use the data to get familiar with those parts of the user interface that deal with return tickets, such as, searching for return tickets.
- Loading the return tickets acts as an end-to-end test of the Oracle Retail Returns Management software installation, from the web services interface up to the back-end database.
- The return ticket data is good sample data that can be used as a starting point for customization and experimentation with data relevant to your organization.

### Using the Returns Data Loader

To use the returns data loader:

1. Change to the db directory.
  - For Oracle Application Server, change to the `<INSTALL_DIR>/returnsmgmt/db` directory.
  - For IBM WebSphere, change to the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
2. If the `returnsManagementDBInstall.jar` file was not expanded as part of the installation, that jar file must be expanded to access the files needed to run the loader.

```
jar xvf returnsmgmtDBInstall.jar
```

3. Edit the part of the `db.properties` file that deals with the returns data loader.

Set the values of the properties as needed. Replace the host name `My_RM_Server` shown in the following example.

```
#####  
# Properties for Returns Seed Data Loading  
#####  
  
# the host name where the seed data should be loaded  
dataLoader.host=My_RM_Server  
  
# the port number where the seed data should be loaded  
# WebSphere App Server 6.x normally uses 9080, JBoss is 8080  
dataLoader.port=9080  
  
# The URL shouldn't need to be modified unless the deployment location moves  
dataLoader.url=http://${dataLoader.host}:${dataLoader.port}/retwebsvc/services/  
ReturnsManager
```

4. Execute the following command:

```
ant load_returns_data
```

About 100 sample return requests and final result messages are sent to the Returns Management server. This step may take several minutes to complete.

This command sends some output to `DataTools.log` in the current directory. Ignore the warning message about attachment support, as the `DataLoader` does not need it to operate properly.

You can view the contents of the submitted XML messages in the `returns-data/tickets` directory. You can also modify the messages and resubmit them by repeating this step.

---

## Appendix: Best Practices for Passwords

This appendix has information on the practices that should be followed for passwords. The following topics are covered:

- ["Password Guidelines"](#)
- ["Special Security Options for Oracle Databases"](#)
- ["Special Security Options for IBM DB2 Databases"](#)

### Password Guidelines

To make sure users and their passwords are properly protected, follow these guidelines. The guidelines are based on the Payment Card Industry Data Security Standard (PCI-DSS):

- Verify the identity of the user before resetting any passwords.
- Set first-time passwords to a unique value for each user and require the password to be changed immediately after the first use.
- Immediately revoke access for any terminated users.
- Remove inactive user accounts at least every 90 days.
- Enable accounts used by vendors for remote maintenance only during the time period when access is needed.
- Communicate password procedures and policies to all users who have access to cardholder data.
- Do not use group, shared, or generic accounts and passwords.
- Require user passwords to be changed at least every 90 days.
- Require a minimum password length of at least seven characters.
- Require that passwords contain both numeric and alphabetic characters.
- Do not accept a new password that is the same as any of the last four passwords used by a user.
- Limit the number of repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or until an administrator enables the user ID.

## Special Security Options for Oracle Databases

The following information is based on Oracle Database version 10.2.0.3.

### Enforcing Password Policies Using Database Profiles

Password policies can be enforced via database profiles. The options can be changed using a SQL statement, for example:

```
alter profile appsample limit
```

Option	Setting	Description
FAILED_LOGIN_ATTEMPTS	4	Maximum number of login attempts before the account is locked.
PASSWORD_GRACE_TIME	3	Number of days a user has to change an expired password before the account is locked.
PASSWORD_LIFE_TIME	90	Number of days that the current password can be used.
PASSWORD_LOCK_TIME	30	Amount of time in minutes that the account is locked.
PASSWORD_REUSE_MAX	10	Number of unique passwords the user must supply before the first password can be reused.
PASSWORD_VERIFY_FUNCTION	<i>&lt;routine_name&gt;</i>	Name of the verification script that is used to ensure that the password meets the requirements of the password policy. See <a href="#">"Enforcing Password Policies Using a Verification Script"</a> .

### Enforcing Password Policies Using a Verification Script

Password policies can be enforced via a password complexity verification script, for example:

```
UTLPWDMG.SQL
```

The password complexity verification routine ensures that the password meets the following requirements:

- Is at least four characters long
- Differs from the user name
- Has at least one alpha, one numeric, and one punctuation mark character
- Is not simple or obvious, such as welcome, account, database, or user
- Differs from the previous password by at least three characters

For example, to set the password to expire as soon as the user logs in for the first time:

```
CREATE USER jbrown  
IDENTIFIED BY zX83yT  
...  
PASSWORD EXPIRE;
```

## Special Security Options for IBM DB2 Databases

The security for DB2 is done at the operating system level. Consult your IBM DB2 documentation for information on creating a security profile that follows the password guidelines.





---

# Appendix: Secure JDBC with Oracle 11g Database

This appendix has information on setting up and communicating with a secured Oracle 11g database server based on the following assumptions:

- Client authentication is not needed.
- The Oracle wallet is used as a trust store on the database server.

SSL encryption for Oracle JDBC has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x, and is supported in the THIN driver starting in 10.2. SSL authentication has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x. The THIN driver supports Oracle Advanced Security SSL implementation in Oracle Database 11g Release 1 (11.1).

For more information, see the following websites:

- [http://www.oracle.com/technology/tech/java/sqlj\\_jdbc/pdf/wp-oracle-jdbc\\_thin\\_ssl.pdf](http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf)
- [http://download.oracle.com/docs/cd/B28359\\_01/network.111/b28530/toc.htm](http://download.oracle.com/docs/cd/B28359_01/network.111/b28530/toc.htm)
- [http://download.oracle.com/docs/cd/B28359\\_01/java.111/b31224/toc.htm](http://download.oracle.com/docs/cd/B28359_01/java.111/b31224/toc.htm)

## Creating the Oracle Wallet and Certificate for the Server

Note the following information:

- The Advanced Security options must be installed with the database server.
- If you want have a user interface, run owm from `$ORACLE_HOME/bin` as oracle.
- The wallet you create must support Auto Login. It must be enabled on the new wallet.
- The following is the wallet directory default:
  - `ORACLE_HOME/admin/ORACLE_SID`
  - Test server wallet information:
    - \* Wallet password: `securedb11g`
    - \* Wallet directory: `/u01/oracle/admin/SECURDB11G`

- When generating a self-signed certificate, note the following:
  - Do not use keytool to create a certificate for using Oracle wallets. They are incompatible.
  - Two wallets are needed to generate a self-signed certificate. One wallet is needed to sign the certificate and another wallet is needed to use the certificate.
  - For command line wallet access, use `orapki`.
  - For instructions on generating a self-signed certificate, see *APPENDIX B CREATING TRUSTSTORES AND KEYSTORES* in the following document:  
[http://www.oracle.com/technology/tech/java/sqlj\\_jdbc/pdf/wp-oracle-jdbc\\_thin\\_ssl.pdf](http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf)
  - The following are examples of `orapki` commands:
    - \* To create the wallet:  

```
orapki wallet create -wallet <wallet directory>
```
    - \* To add the self-signed certificate:  

```
orapki wallet add -wallet <wallet directory> -dn  
CN=<certificate name>,C-US -keysize 2048 -self_signed -validity 3650
```
    - \* To view the wallet:  

```
orapki wallet display -wallet <wallet directory>
```
- The Wallet Manager UI can also be used to import certificates.

## Securing the Listener on the Server

The `listener.ora`, `tnsnames.ora`, and `sqlnet.ora` files are found in the `$ORACLE_HOME/network/admin` directory. If the `sqlnet.ora` file does not exist, you need to create it.

To secure the listener on the server:

1. Add TCPS protocol to the `listener.ora` file.
2. Add TCPS protocol to the `tnsnames.ora` file.
3. Add the Oracle Wallet location to the `sqlnet.ora` and `listener.ora` files.
4. Add disabling of client authentication to the `sqlnet.ora` and `listener.ora` files.
5. Add encryption-only cipher suites to the `sqlnet.ora` file.
6. Bounce the listener once the file is updated.

## Examples of Network Configuration Files

Examples of the following network configuration files are shown in this section:

- [listener.ora](#)
- [sqlnet.ora](#)
- [tnsnames.ora](#)

## listener.ora

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/oracle/11g)
      (PROGRAM = extproc)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = 10.143.44.108) (PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS) (HOST = 10.143.44.108) (PORT = 2484))
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROCO))
    )
  )

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))

SSL_CLIENT_AUTHENTICATION=FALSE
```

---

---

**Caution:** To generate a trace log, add the following entries to the listener.ora file:

```
TRACE_LEVEL_LISTENER = ADMIN
TRACE_DIRECTORY_LISTENER = /u01/oracle/11g/network/trace
TRACE_FILE_LISTENER = listener.trc
```

---

---

## sqlnet.ora

```
SSL_CLIENT_AUTHENTICATION=FALSE

SSL_CIPHER_SUITES=(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_
MD5, SSL_DH_anon_WITH_DES_CBC_SHA)

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))
```

## tnsnames.ora

```
SECURDB11G =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = 10.143.44.108) (PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS) (HOST = 10.143.44.108) (PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = SECURDB11G)
    )
  )
```

## Securing Client Access

---

**Caution:** Ensure you are using `ojdbc.jar` version 10.2.x or later. Version 10.1.x or earlier will not connect over TCPS.

---

To secure client access:

1. Export the self-signed certificate from the server Oracle Wallet and import it into a local trust store.

2. Use the following URL format for the JDBC connection:

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (HOST=10.143.44.108)
(PORT=2484) ) (CONNECT_DATA= (SERVICE_NAME=SECURDB11G)))
```

3. The database connection call requires the following properties to be set, either as system properties or JDBC connection properties:

Property	Value
oracle.net.ssl_cipher_suites	(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_SHA)
javax.net.ssl.trustStore	Path and file name of trust store For example: /DevTools/Testing/Secure11g/truststore/truststore
javax.net.ssl.trustStoreType	JKS
javax.net.ssl.trustStorePassword	Password for trust store

## Specific Instructions for Central Office

Complete the following steps.

### Configuring the Application Server Machine

To configure the application server machine, note the following:

- As a client, the application server machine needs to have the trusted certificate added to a local trust store. Follow the previous instructions for exporting the known certificate and importing it to a local trust store.

This is not required as Release 13.1 Oracle Retail Central Office uses Diffie-Hellman anonymous authentication. With Diffie-Hellman anonymous authentication, neither the server nor the client will be authenticated.

- Oracle Application Server 10.1.3.4 is using the `ojdbc14.jar` file for 10.1.0.5 which does not support the SSL protocol. You need to update the JDBC driver to a 10.2.0.3 version.

- For information on securing a website, see the following website:  
[http://download.oracle.com/docs/cd/B31017\\_01/web.1013/b28957/configssl.htm#CHDHGCDJ](http://download.oracle.com/docs/cd/B31017_01/web.1013/b28957/configssl.htm#CHDHGCDJ)
- The following instructions describe creating a JDBC shared lib for application. By default, Oracle Application Server 10.1.3.4 comes up with JDBC drivers but they do not support TCPS protocol. TCPS is supported in database version 10.2.0.3.  
 For information on creating a secure JDBC shared library, see the following website:  
[http://download.oracle.com/docs/cd/B31017\\_01/web.1013/b28221/servdats005.htm#BABCEDIG](http://download.oracle.com/docs/cd/B31017_01/web.1013/b28221/servdats005.htm#BABCEDIG)

## Securing the Data Source

To edit the data source definition in `<instance>/config/data-sources.xml`:

1. Update the URL to use the expanded Oracle format:

```
*** (ex. jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps)
(HOST=10.143.44.108) (PORT=2484) ) (CONNECT_DATA= (SERVICE_NAME=SECURDB11G)))
```

2. Add the SSL JDBC properties. The following example shows part of the `data-sources.xml` file.

```
<connection-pool name="Oracle11GPool">
  <connection-factory factory-class="oracle.jdbc.pool.OracleDataSource"
user="securuser" password="->securuser"

url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps) (HOST=10.143.44.108
) (PORT=2484)) (CONNECT_DATA=(SERVICE_NAME=SECURDB11G))) ">
  <connection-properties>
    <property name="oracle.net.ssl_cipher_suites"
      value="(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_
RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_SHA)"/>
  </connection-properties>
</connection-factory>
</connection-pool>
```

## Creating a JDBC Shared Library for the Application

To create the library:

1. Create a directory in `$ORACLE_HOME/j2ee/home/shared-lib/oracle.jdbc` for the new Oracle JDBC driver shared library. For example, create the following folder:

```
$ORACLE_HOME/j2ee/home/shared-lib/oracle.jdbc/10.3
```

You reference the actual Oracle JDBC driver jar file relative to this directory. You can either put the Oracle JDBC driver jar file (`ojdbc14.jar`) from the database into this directory and simply reference the jar file by name, or put it into some other directory and reference the jar file with a partial path relative to this directory.

2. Define the new Oracle JDBC driver shared library and TopLink shared library in the `server.xml` file.

```
<shared-library name="oracle.jdbc" version="10.3">
<code-source path="ojdbc14.jar"/>
</shared-library>
<shared-library name="oracle.toplink" version="10.3" library-compatible="true">
<code-source path="../../../toplink/jlib/toplink.jar"/>
<code-source path="../../../toplink/jlib/antlr.jar"/>
<code-source path="../../../toplink/jlib/cciblackbox-tx.jar"/>
<import-shared-library name="oc4j.internal"/>
<import-shared-library name="oracle.xml"/>
<import-shared-library name="oracle.jdbc" max-version="10.3"/>
<import-shared-library name="oracle.dms"/>
</shared-library>
```

3. Import your new shared libraries for your application. To make the new `oracle.jdbc` and `oracle.toplink` shared libraries the default for all applications in your OC4J instance, update the `system-applications.xml` file as shown in the following example.

```
<imported-shared-libraries>
  <import-shared-library name="oracle.jdbc" min-version="10.3"
max-version="10.3"/>
  <import-shared-library name="oracle.toplink" min-version="10.3"
max-version="10.3"/>
</imported-shared-libraries>
```

---

## Appendix: Secure JDBC with IBM DB2

This appendix has information on how to enable SSL for IBM DB2. Information from the DB2 V9 Information Center, *Global Security Kit Secure Sockets Layer Introduction*, and *iKeyman User's Guide* is included in this appendix.

IBM DB2 has supported SSL encryption since version 9.1 Fix Pack 3. Information on how to configure SSL on the server and client can be found at the following websites:

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0025241.htm>
- <http://www-1.ibm.com/support/docview.wss?uid=swg21249656>

### Summary

To secure JDBC on IBM DB2 requires the following:

- An SSL provider must be established on the DB2 server.
- The provider requires a digital certificate and corresponding private key to provide the secure communications.
- The client either needs to have a copy of the digital certificate or trust the signer of the server certificate.
- The client needs to be configured to use the secure service, and optionally use a FIPS-compliant SSL provider.

### Prerequisites

The information in this section is from the DB2 V9 Information Center.

1. Make sure you have the required fix pack version of DB2.

To determine the fix pack level you have, run the `db2level` command at the command line. If you have Version 9.1 with a fix pack version earlier than Fix Pack 3, you need to obtain Fix Pack 3 or a later version.

2. Make sure the GSKit is installed.

On linux, it is located in `/usr/local/ibm/gsk7`.

3. Make sure the GSKit libraries are in the path.

Make sure the `/usr/local/ibm/gsk7/lib` directory is included in `LD_LIBRARY_PATH`.

4. For information on how to check if the connection concentrator is in use, see the IBM documentation.

## Setting up the Key Store

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

1. If you are not already logged in to the server, log in as the instance owner.
2. Start iKeyman GUI gsk7ikm.  
If the Java Cryptographic Extension(JCE) files were not found, make sure the JAVA\_HOME environment variable points to a JDK that contains the JCE.
3. Click **Key Database File** and then **New**.
4. Select a key database type, filename, and location.  
It is suggested that a CMS key database is created. This is consistent with the DB2 Infocenter example. For example:  

```
/home/db2inst1/GSKit/Keystore/key.kdb
```
5. Click **OK**. The Password Prompt window is displayed.
6. Enter a password for the key database.
7. Click **OK**. A confirmation window is displayed. Click **OK**.

## Creating a Self-signed Digital Certificate for Testing

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

1. If you are not already logged in to the server, log in as the instance owner.
2. Start iKeyman GUI gsk7ikm.  
If the Java Cryptographic Extension(JCE) files were not found, make sure the JAVA\_HOME environment variable points to a JDK that contains the JCE.
3. Click **Key Database File** and then **Open**.
4. Select the key database file where you want to add the self-signed digital certificate.
5. Click **Open**. The Password Prompt window is displayed.
6. Select **Personal Certificates** from the menu.
7. Click **New Self-Signed**. The Create New Self-Signed Certificate Window is displayed.
8. Type a Key Label, such as `keytest`, for the self-signed digital certificate.
9. Type a **Common Name and Organization**, and select a **Country**. For the remaining fields, accept the default values or enter new values.
10. Click **OK**. The IBM Key Management Window is displayed. The Personal Certificates field shows the name of the self-signed digital certificate you created.

## Configuring the IBM DB2 Server

The information in this section is from the DB2 V9 Information Center.

1. If you are not already logged in to the server, log in as the instance owner.



## 2. Create an SSL configuration file:

- For Linux and UNIX:

<INSTHOME>/cfg/SSLconfig.ini

For example:

/home/db2inst1/sqllib/cfg/SSLconfig.ini

- For Windows:

<INSTHOME>\SSLconfig.ini

For example:

F:\IBM\SQLLIB\DB2\SSLconfig.ini

<INSTHOME> is the home directory of the instance.

---

**Caution:** It is recommended that you set the file permission to limit access to the `SSLconfig.ini`, as the file might contain sensitive data. For example, limit read and write authority on the file to members of the SYSADM group if the file contains the password for Key Store.

---

3. Add SSL parameters to the SSL configuration file. The `SSLconfig.ini` file contains the SSL parameters that are used to load and start SSL. The list of SSL parameters are shown in the following table:

SSL parameter name	Description
DB2_SSL_KEYSTORE_FILE	Fully qualified file name of the Key Store that stores the Server Certificate.
DB2_SSL_KEYSTORE_PW	Password of the Key Store that stores the Server Certificate.
DB2_SSL_KEYSTORE_LABEL	Label for the Server Certificate. If it is omitted, the default certificate for the Key Store is used.
DB2_SSL_LISTENER	Service name or port number for the SSL listener.

The following is an example of an `SSLconfig.ini` file:

```
DB2_SSL_KEYSTORE_FILE=/home/db2inst1/GSKit/Keystore/key.kdb
DB2_SSL_LISTENER=20397
DB2_SSL_KEYSTORE_PW=abcd1234
```

4. Add the value SSL to the DB2COMM registry variable. For example, use the following command:

```
db2set -i <db2inst1> DB2COMM=SSL
```

where <db2inst1> is the IBM DB2 instance name.

The database manager can support multiple protocols at the same time. For example, to enable both TCP/IP and SSL communication protocols:

```
db2set -i <db2inst1> DB2COMM=SSL,TCPIP
```

5. Restart the IBM DB2 instance. For example, use the following commands:

```
db2stop
```

```
db2start
```

At this point, the server should be ready to start serving SSL connections. You can check the `db2diag.log` file for errors. There should be no errors pertaining to SSL after the restart.

## Exporting a Certificate from iKeyman

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

In order to be able to talk to the server, the clients need to have a copy of the self-signed certificate from the server.

1. Start iKeyman. The IBM Key Management window is displayed.
2. Click **Key Database File** and then **Open**. The Open window is displayed.
3. Select the source key database. This is the database that contains the certificate you want to add to another database as a signer certificate.
4. Click **Open**. The Password Prompt window is displayed.
5. Enter the key database password and click **OK**. The IBM Key Management window is displayed. The title bar shows the name of the selected key database file, indicating that the file is open and ready.
6. Select the type of certificate you want to export: Personal or Signer.
7. Select the certificate that you want to add to another database.
  - If you selected Personal, click **Extract Certificate**.
  - If you selected Signer, click **Extract**.

The Extract a Certificate to a File window is displayed.

8. Click **Data type** and select a data type, such as Base64-encoded ASCII data. The data type needs to match the data type of the certificate stored in the certificate file. The iKeyman tool supports Base64-encoded ASCII files and binary DER-encoded certificates.
9. Enter the certificate file name and location where you want to store the certificate, or click **Browse** to select the name and location.
10. Click **OK**. The certificate is written to the specified file, and the IBM Key Management window is displayed.

## Configuring the IBM FIPS-compliant Provider for SSL (optional)

The information in this section is from the DB2 V9 Information Center.

The Sun JSSE SSL provider works with the IBM DB2 driver by following the above instructions. If you want to use the IBM FIPS-compliant provider, you have to use the IBM JDK and make the following configuration changes.

---

**Note:** If you are following the IBM documentation, note the following issues:

- Prior to the numbered steps, it says to add several lines to `java.security`. Do not add the lines.
  - Step two incorrectly shows setting `ssl.SocketFactory.provider` twice. It only needs to be done once.
- 

1. Set the `IBMJSSE2 FIPS` system property to enable FIPS mode:

```
com.ibm.jsse2.JSSEFIPS=true
```

2. Set security properties to ensure that all JSSE code uses the `IBMJSSE2` provider. The following example shows the entries in `java.security`.

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

3. Add the `IBMJCEFIPS` cryptographic provider.

Add `com.ibm.crypto.fips.provider.IBMJCEFIPS` to the provider list before the `IBMJCE` provider. Do not remove the `IBMJCE` provider. The `IBMJCE` provider is required for Key Store support.

The following example shows the entries in `java.security`.

```
# List of providers and their preference orders (see above):
#
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
# inserted provider 2 for FIPS
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
```

## Configuring Central Office on IBM WebSphere

It is difficult to configure Oracle Retail Central Office to use secure JDBC from the start by using the URL that includes the `sslConnection` property and secure port number. The following instructions are for retrofitting it into the configuration after the install is complete.

To complete the configuration:

1. Install the database digital certificate into the application server truststore.
  - a. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  - b. Expand the Security menu.
  - c. Click the **SSL certificate and key management** option.
  - d. In the Related Items list, click **Key stores and certificates**.
  - e. Click the **NodeDefaultTrustStore** link in the list.
  - f. In the Additional Properties list, click the **Signer certificates** link.
  - g. Click the **Add** button.

- h. Enter a distinct alias and the full path to the certificate file on the server in the File name field. Make sure the Data type corresponds to the type in the file. The certificate should appear in the list of Signer certificates.
2. Update all the data sources to use SSL. (jdbc/DataSource, jdbc/DimpDataSource, jdbc/DimpDataSource)
  - a. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  - b. Expand the Resources menu option.
  - c. Expand the JDBC menu option.
  - d. Click the **Data sources** option. The list of data sources is displayed.
  - e. Click on the data source to be edited.
  - f. In the Additional Properties list, click the **Custom properties** link.
  - g. Click the **New** button.
  - h. Enter sslConnection in the Name field, true in the Value field, and click **OK**.
  - i. Click the data source name in the bread crumb trail to return to the data source edit page.
  - j. Change the Port number field from the TCPIP port to the SSL port.
  - k. Click **OK**.
  - l. Edit the remaining data sources.
  - m. Save the configuration.
3. Stop the server.
4. Edit the custom user registry properties in customRegistry.properties.
  - a. Change the JDBC URL to use the SSL port.
  - b. Append :sslConnection=true; to the end.
5. Start the server.

## Useful Links

For more information, see the following websites:

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.apdv.java.doc/doc/rjvdsprp.htm>

This website has documentation of all the properties available in the DB2 Driver for JDBC.

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.apdv.java.doc/doc/tjvjcccn.htm>

This website contains documentation of the URL syntax for connecting to DB2 using JDBC.

- <http://www.redbooks.ibm.com/abstracts/sq247555.html>

An IBM Redbook on security related issues with DB2, including auditing and data encryption. The IBM Form Number is SG24-7555-00.

---

## Appendix: Installation Order

This appendix provides a guideline for the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use only some of the applications, the order is still valid, less the applications not being installed.

### Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM), Oracle Retail Sales Audit (ReSA)
2. Oracle Retail Service Layer (RSL)
3. Oracle Retail Extract, Transform, Load (RETL)
4. Oracle Retail Active Retail Intelligence (ARI)
5. Oracle Retail Warehouse Management System (RWMS)
6. Oracle Retail Allocation
7. Oracle Retail Invoice Matching (ReIM)
8. Oracle Retail Price Management (RPM)

---

**Note:** During installation of RPM, you are asked for the RIBforRPM provider URL. Since RIB is installed after RPM, make a note of the URL you enter. If you need to change the RIBforRPM provider URL after you install RIB, you can do so by editing the `jndi_provider.xml` file.

---

9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO) or Back Office with Labels and Tags (ORLAT)
12. Oracle Retail Store Inventory Management (SIM)

---

**Note:** During installation of SIM, you are asked for the AIP provider URL. Since AIP is installed after SIM, make a note of the URL you enter. If you need to change the AIP provider URL after you install AIP, you can do so by editing the `jndi_providers_ribclient.xml` file.

---

13. Oracle Retail Predictive Application Server (RPAS)

- 14.** Oracle Retail Merchandise Financial Planning (MFP)
- 15.** Oracle Retail Size Profile Optimization (SPO)
- 16.** Oracle Retail Assortment Planning (AP)
- 17.** Oracle Retail Item Planning (IP)
- 18.** Oracle Retail Item Planning configured for COE (IPCOE)
- 19.** Oracle Retail Advanced Inventory Planning (AIP)
- 20.** Oracle Retail Integration Bus (RIB)
- 21.** Oracle Retail Point-of-Service (ORPOS)
- 22.** Oracle Retail Analytics Applications
- 23.** Oracle Retail Data Warehouse (RDW)
- 24.** Oracle Retail Workspace (ORW)